

## 明 細 書

サービス不能攻撃防御方法、サービス不能攻撃防御システム、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラム

### 技術分野

[0001] この発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくはこの中継装置で通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法、サービス不能攻撃防御システム、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムに関し、特に、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御システム、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムに関する。

### 背景技術

[0002] 従来、ネットワークを介した攻撃としてサービス不能攻撃および分散型サービス不能攻撃 (Distributed Denial of Service Attack、以下単に「DDos攻撃」と言う) が知られている。かかるDDos攻撃から通信機器を防御する分散型サービス不能攻撃防御システムでは、攻撃対象となる通信機器とネットワークとの間に設けられたゲートウェイ装置やネットワークを構成するルータ装置がパケットを制限することになる。具体的には、ネットワークを介して通信機器に向けて送信されたパケットを正規パケット、容疑パケットまたは不正パケットに分類し、通信機器に送信されるパケットを制限していた(例えば、特許文献1参照)。

[0003] このような従来の分散型サービス不能攻撃防御システムにおいては、あらかじめ登録された攻撃検知条件に基づいてゲートウェイ装置が攻撃を検知すると、攻撃検知されたパケットの特徴を示す容疑シグネチャが生成され、生成された容疑シグネチャがネットワークを構成するルータ装置等の中継装置に通知される。

[0004] 一方、容疑シグネチャに当てはまるパケットのうち通信機器に対する攻撃とみなされないパケット(以下「非攻撃パケット」と言う)の特徴を表す正規シグネチャが、あらかじめ登録された正規条件情報に基づいてゲートウェイ装置によって生成され、生成された正規シグネチャがネットワークを構成するルータ装置等の中継装置に通知される。

[0005] 容疑シグネチャおよび正規シグネチャが通知された中継装置並びにゲートウェイ装置によって中継されるパケットは、容疑シグネチャおよび正規シグネチャに基づいてシェーピングやフィルタリング等の処理が施される。

[0006] このように、従来の分散型サービス不能攻撃防御システムは、攻撃を行うパケットの通過を出来るだけ攻撃元の近くで制限することによって、攻撃を行うパケット(以下「攻撃パケット」と言う)による悪影響を出来るだけ小さくしている。

[0007] 特許文献1:特開2003-283554号公報

発明の開示

発明が解決しようとする課題

[0008] しかしながら、従来の分散型サービス不能攻撃防御システムにおいては、攻撃から防御する対象の通信機器に対する非攻撃パケットの条件を表す正規条件情報の追加や変更等の管理がゲートウェイ装置のオペレータによって行われるため、正規条件情報の管理が煩雑になるといった課題があった。

[0009] 本発明は、上述した従来技術による問題点を解消するためになされたものであり、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御システム、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムを提供することを目的とする。

課題を解決するための手段

[0010] 上述した課題を解決し、目的を達成するため、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記ネットワーク上に所在する正当な装置が非攻撃パケットの送信元を示す正規アドレス情報を発行し、前記ゲート装置が前記正当な装置が発

行した正規アドレス情報に基づいて前記通信機器へ攻撃をおこなうパケットの通過を制限することを特徴とする。

[0011] この発明によれば、ネットワーク上に所在する正当な装置が非攻撃パケットの送信元を示す正規アドレス情報を発行し、ゲート装置が正当な装置が発行した正規アドレス情報に基づいて通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、通信機器に対するサービス不能攻撃を効率的に防御することができる。

[0012] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が取得する正規アドレス情報取得工程と、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて前記ゲート装置が非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ゲート装置が前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする。

[0013] この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が取得し、取得した正規アドレス情報に基づいてゲート装置が非攻撃パケットの条件を示す正規条件情報を生成し、ゲート装置がネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。

[0014] また、本発明は、上記発明において、前記正規アドレス情報取得工程は、前記ゲート装置が前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知工程と、前記中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記アドレス情報通知工程により通知された前記アドレス情報に基づいて当該正

規アドレス情報を前記ゲート装置に対して中継する正規アドレス情報中継工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする。

[0015] この発明によれば、ゲート装置が中継装置に対して自装置のアドレス情報を通知し、中継装置が正当な装置からの正規アドレス情報を受信した場合に、通知されたアドレス情報に基づいて当該正規アドレス情報をゲート装置に対して中継し、ゲート装置が正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

[0016] また、本発明は、上記発明において、前記アドレス情報通知工程は、前記ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置に前記ゲート装置のアドレス情報を中継し、前記正規アドレス情報中継工程は、前記他の中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記ゲート装置のアドレス情報に基づいて隣接する中継装置若しくは前記ゲート装置に前記正規アドレス情報を中継することを特徴とする。

[0017] この発明によれば、ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置にゲート装置のアドレス情報を中継し、他の中継装置が正当な装置からの正規アドレス情報を受信した場合に、ゲート装置のアドレス情報に基づいて隣接する中継装置若しくはゲート装置に前記正規アドレス情報を中継することとしたので、必要な各中継装置を経由しつつ効率良く正規アドレス情報をゲート装置まで中継することができる。

[0018] また、本発明は、上記発明において、前記正規アドレス情報取得工程は、正規アドレス情報を一括管理する正規アドレス情報提供装置が前記正規アドレス情報を各正当な装置から受信して格納する正規アドレス情報格納工程と、前記正規アドレス情報提供装置が前記ゲート装置から前記正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報を前記ゲート装置に対して通知する正規アドレス情報通知工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする。

- [0019] この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置が正規アドレス情報を各正当な装置から受信して格納しておき、この正規アドレス情報提供装置がゲート装置から正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報をゲート装置に対して通知し、ゲート装置が正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。
- [0020] また、本発明は、上記発明において、前記正規アドレス情報取得工程は、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器により送信された前記正規アドレス情報を前記ゲート装置が取得することを特徴とする。
- [0021] この発明によれば、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器をネットワーク上に所在する正当な装置とみなして、これらから送信された正規アドレス情報をゲート装置が取得することとしたので、正当な装置から受信した正しい正規アドレス情報に基づく正規条件情報を生成でき、不正な攻撃を看過する事態を防ぐことができる。
- [0022] また、本発明は、上記発明において、前記ゲート装置が前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知工程と、前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記正規条件情報生成工程により生成された正規条件情報を正規条件情報記憶部に格納する正規条件情報格納工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程とをさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。
- [0023] この発明によれば、ゲート装置がネットワークから受信されたパケットによる攻撃を検知し、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成し、正規条件情

報を正規条件情報記憶部に格納し、容疑シグネチャに該当するパケットのうち正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという従来の指標を利用しつつ効率良く攻撃パケットの通過を制限することができる。

[0024] また、本発明は、上記発明において、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に通知するシグネチャ通知工程と、前記中継装置が前記シグネチャ通知工程により通知された容疑シグネチャおよび正規シグネチャに基づいてパケットの通過を制限制御するパケット制限制御工程とをさらに含んだことを特徴とする。

[0025] この発明によれば、容疑シグネチャおよび正規シグネチャをゲート装置が中継装置に通知し、通知された容疑シグネチャおよび正規シグネチャに基づいて中継装置がパケットの通過を制限制御することとしたので、中継装置においても効率良く攻撃パケットの通過を制限することができる。

[0026] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記ネットワークから受信されたパケットによる攻撃を前記ゲート装置が検知する攻撃検知工程と、前記攻撃検知工程により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が前記中継装置から取得する正規アドレス情報取得工程と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御を前記ゲート装置がおこなう通過制御工程とを含んだことを特徴とする。

[0027] この発明によれば、ネットワークから受信されたパケットによる攻撃をゲート装置が検知し、通信機器への攻撃が検知された場合に、ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が中継

装置から取得し、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

- [0028] また、本発明は、上記発明において、前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを前記ゲート装置が生成する容疑シグネチャ生成工程をさらに含み、前記正規アドレス情報取得工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする。
- [0029] この発明によれば、攻撃が検知されたパケットの特徴を表す容疑シグネチャをゲート装置が生成し、生成された容疑シグネチャを中継装置に送信し、その結果返信された正規アドレス情報を取得するよう構成したので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。
- [0030] また、本発明は、上記発明において、前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする。
- [0031] この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち、生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

- [0032] また、本発明は、上記発明において、前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報生成工程により生成された正規条件情報に示される条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。
- [0033] この発明によれば、容疑シグネチャに該当するパケットのうち、生成された正規条件情報に示される条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成した容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。
- [0034] また、本発明は、上記発明において、前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に転送するシグネチャ転送工程をさらに含んだことを特徴とする。
- [0035] この発明によれば、生成された正規シグネチャをゲート装置が中継装置に転送することとしたので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。
- [0036] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記ゲート装置は、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴と

する。

- [0037] この発明によれば、ゲート装置は、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得し、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。
- [0038] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記ゲート装置は、前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、前記攻撃検知手段により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手段と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とする。
- [0039] この発明によれば、ゲート装置は、ネットワークから受信されたパケットによる攻撃を検知し、攻撃が検知された場合に、ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を中継装置から取得し、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。
- [0040] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象

となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置であって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする。

[0041] この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得し、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。

[0042] また、本発明は、上記発明において、前記正規アドレス情報取得手段は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手段と、前記アドレス情報通知手段により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手段とを備えたことを特徴とする。

[0043] この発明によれば、中継装置に対して自装置のアドレス情報を通知し、通知した自装置のアドレス情報に応答して中継装置が返送した正当な装置からの正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

[0044] また、本発明は、上記発明において、前記正規アドレス情報取得手段は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手段と、前記正規アドレス情報の送

信要求に応答して返送された正規アドレス情報を受信する受信手段とを備えたことを特徴とする。

[0045] この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して正規アドレス情報の送信要求をおこない、この正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。

[0046] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置であって、前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、前記攻撃検知手段により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手段と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とする。

[0047] この発明によれば、ネットワークから受信されたパケットによる攻撃を検知し、通信機器への攻撃が検知された場合に、ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を中継装置から取得し、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、ゲート装置が攻撃を検知すると各中継装置が保持する正規アドレス情報を自動的に取得することができるので、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

[0048] また、本発明は、上記発明において、前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段をさらに備

え、前記正規アドレス情報取得手段は、前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする。

[0049] この発明によれば、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成し、生成された容疑シグネチャを中継装置に送信し、その結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

[0050] また、本発明は、上記発明において、前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段と備えたことを特徴とする。

[0051] この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

[0052] また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、前記ゲート装置のアドレス情報を取得するアドレス情報取得手段と、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手段により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手段とを備えたことを特徴とする。

[0053] この発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報

を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を中継することとしたので、効率良く正規アドレス情報をゲート装置まで中継することができる。

[0054] また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、前記ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段とを備えたことを特徴とする。

[0055] この発明によれば、ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶し、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を攻撃を検知したゲート装置に転送することとしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

[0056] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置に用いるゲート装置用プログラムであって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手順と、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパ

ケット制限手順とをコンピュータに実行させることを特徴とする。

- [0057] この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得し、取得した正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。
- [0058] また、本発明は、上記発明において、前記正規アドレス情報取得手順は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手順と、前記アドレス情報通知手順により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手順とを含んだことを特徴とする。
- [0059] この発明によれば、中継装置に対して自装置のアドレス情報を通知し、通知した自装置のアドレス情報に応答して中継装置が返送した正当な装置からの正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。
- [0060] また、本発明は、上記発明において、前記正規アドレス情報取得手順は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手順と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手順とを含んだことを特徴とする。
- [0061] この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して正規アドレス情報の送信要求をおこない、この正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。
- [0062] また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象

となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置に用いるゲート装置用プログラムであって、前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手順と、前記攻撃検知手順により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手順と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手順とをコンピュータに実行させることを特徴とする。

[0063] この発明によれば、ネットワークから受信されたパケットによる攻撃を検知し、通信機器への攻撃が検知された場合に、ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を中継装置から取得し、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、ゲート装置が攻撃を検知すると各中継装置が保持する正規アドレス情報を自動的に取得することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

[0064] また、本発明は、上記発明において、前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順をさらに含み、前記正規アドレス情報取得手順は、前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする。

[0065] この発明によれば、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成し、生成された容疑シグネチャを中継装置に送信し、その結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

[0066] また、本発明は、上記発明において、前記通過制御手順は、前記正規アドレス情

報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする。

[0067] この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

[0068] また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、前記ゲート装置のアドレス情報を取得するアドレス情報取得手順と、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手順により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手順とをコンピュータに実行させることを特徴とする。

[0069] この発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を中継することとしたので、効率良く正規アドレス情報をゲート装置まで中継することができる。

[0070] また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、前記ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手順と、前記ゲート装置により前記通信機器

への攻撃が検知された場合に、前記正規アドレス情報記憶手順に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順とをコンピュータに実行させることを特徴とする。

- [0071] この発明によれば、ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶し、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を攻撃を検知したゲート装置に転送することとしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

#### 発明の効果

- [0072] 本発明によれば、ネットワーク上に所在する正当な装置が非攻撃パケットの送信元を示す正規アドレス情報を発行し、ゲート装置が正当な装置が発行した正規アドレス情報に基づいて通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、通信機器に対するサービス不能攻撃を効率的に防御することができる。
- [0073] また、本発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が取得し、取得した正規アドレス情報に基づいてゲート装置が非攻撃パケットの条件を示す正規条件情報を生成し、ゲート装置がネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規条件情報を効率良く生成することができ、もってゲート装置のオペレータによる正規条件情報の管理負担を軽減することができる。
- [0074] また、本発明によれば、ゲート装置が中継装置に対して自装置のアドレス情報を通知し、中継装置が正当な装置からの正規アドレス情報を受信した場合に、通知されたアドレス情報に基づいて当該正規アドレス情報をゲート装置に対して中継し、ゲー

ト装置が正規アドレス情報を受信するよう構成したので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

- [0075] また、本発明によれば、ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置にゲート装置のアドレス情報を中継し、他の中継装置が正当な装置からの正規アドレス情報を受信した場合に、ゲート装置のアドレス情報に基づいて隣接する中継装置若しくはゲート装置に前記正規アドレス情報を中継するよう構成したので、必要な各中継装置を経由しつつ効率良く正規アドレス情報をゲート装置まで中継することができる。
- [0076] また、本発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置が正規アドレス情報を各正当な装置から受信して格納しておき、この正規アドレス情報提供装置がゲート装置から正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報をゲート装置に対して通知し、ゲート装置が正規アドレス情報を受信するよう構成したので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。
- [0077] また、本発明によれば、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器をネットワーク上に所在する正当な装置とみなして、これらから送信された正規アドレス情報をゲート装置が取得するよう構成したので、正当な装置から受信した正しい正規アドレス情報に基づく正規条件情報を生成でき、不正な攻撃を看過する事態を防ぐことができる。
- [0078] また、本発明によれば、ゲート装置がネットワークから受信されたパケットによる攻撃を検知し、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成し、正規条件情報を正規条件情報記憶部に格納し、容疑シグネチャに該当するパケットのうち正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという従来の指標を利用しつつ効率良く攻撃パケットの通過を制限すること

ができる。

- [0079] また、本発明によれば、容疑シグネチャおよび正規シグネチャをゲート装置が中継装置に通知し、通知された容疑シグネチャおよび正規シグネチャに基づいて中継装置がパケットの通過を制限制御するよう構成したので、中継装置においても効率良く攻撃パケットの通過を制限することができる。
- [0080] また、本発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を通知するよう構成したので、効率良く正規アドレス情報をゲート装置まで通知することができる。
- [0081] また、本発明によれば、ネットワークから受信されたパケットによる攻撃をゲート装置が検知し、通信機器への攻撃が検知された場合に、ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が中継装置から取得し、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。
- [0082] また、本発明によれば、攻撃が検知されたパケットの特徴を表す容疑シグネチャをゲート装置が生成し、生成された容疑シグネチャを中継装置に送信し、その結果返信された正規アドレス情報を取得するよう構成したので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。
- [0083] また、本発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち、生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機

器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

[0084] また、本発明によれば、容疑シグネチャに該当するパケットのうち、生成された正規条件情報に示される条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成した容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。

[0085] また、本発明によれば、生成された正規シグネチャをゲート装置が中継装置に転送することとしたので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。

[0086] また、本発明によれば、ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶し、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を攻撃を検知したゲート装置に転送することとしたので、各中継装置が保持する正規アドレス情報を、攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

#### 図面の簡単な説明

[0087] [図1]図1は、本実施例1に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

[図2]図2は、図1に示したゲート装置の構成を示すブロック図である。

[図3]図3は、本実施例1に係る攻撃検知条件の一例を示す図である。

[図4]図4は、本実施例1に係る正規条件情報の一例を示す図である。

[図5]図5は、本実施例1に係る不正条件の一例を示す図である。

[図6]図6は、図1に示した中継装置の構成を示すブロック図である。

[図7]図7は、図2に示したゲート装置の攻撃検知動作を示すフローチャートである。

[図8]図8は、図6に示した中継装置のシグネチャ受信動作を示すフローチャートである。

[図9]図9は、図2に示したゲート装置のパケット制限動作を示すフローチャートである。

[図10]図10は、本実施例1に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

[図11]図11は、本実施例2に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

[図12]図12は、図11に示したゲート装置の構成を示すブロック図である。

[図13]図13は、図11に示した中継装置の構成を示すブロック図である。

[図14]図14は、本実施例2に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

[図15]図15は、本実施例3に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

[図16]図16は、図15に示したゲート装置の構成を示すブロック図である。

[図17]図17は、本実施例3に係る攻撃検知条件の一例を示す図である。

[図18]図18は、本実施例3に係る正規条件情報の一例を示す図である。

[図19]図19は、本実施例3に係る不正条件の一例を示す図である。

[図20]図20は、図15に示した中継装置の構成を示すブロック図である。

[図21]図21は、図16に示したゲート装置の攻撃検知動作を示すフローチャートである。

[図22]図22は、図20に示した中継装置のシグネチャ受信動作を示すフローチャートである。

[図23]図23は、図16に示したゲート装置のパケット制限動作を示すフローチャートである。

[図24]図24は、本実施例3に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

## 符号の説明

- [0088] 1、50 分散型サービス不能攻撃防御システム
- 2 ネットワーク
- 3、4、5、6、53、54、55、56 中継装置
- 7 通信機器
- 8、58 ゲート装置
- 9 LAN
- 10、60 アドレス発行サーバ
- 11 エッジルータ
- 12、13、15、16 通信機器
- 14 LAN
- 20 攻撃検知部
- 21 容疑シグネチャ生成部
- 22 正規条件情報格納部
- 23、73 正規条件情報生成部
- 24 正規シグネチャ生成部
- 25、35 不正シグネチャ生成部
- 26、36 パケット制限部
- 27、77 シグネチャ通知部
- 37、87 シグネチャ中継部
- 28 ネットワークインタフェース
- 30 入力ポート
- 31 スイッチ
- 32 出力ポート
- 38 アドレス情報記憶部
- 39 正規アドレス情報送信部
- 59 正規アドレス情報記憶装置
- 101 分散型サービス不能攻撃防御システム

- 102 ネットワーク
- 103、104、105、106 中継装置
- 107 通信機器
- 108 ゲート装置
- 109 LAN
- 110 アドレス発行サーバ
- 111 エッジルータ
- 112、113、115、116 通信機器
- 114 LAN
- 120 攻撃検知部
- 121 容疑シグネチャ生成部
- 122 正規条件情報格納部
- 123 正規条件情報生成部
- 124 正規シグネチャ生成部
- 125、135 不正シグネチャ生成部
- 126、136 パケット制限部
- 127、137 シグネチャ転送部
- 128 ネットワークインタフェース
- 130 入力ポート
- 131 スイッチ
- 132 出力ポート
- 138 アドレス情報記憶部
- 139 正規アドレス情報送信部

#### 発明を実施するための最良の形態

[0089] 以下に添付図面を参照して、この発明に係るサービス不能攻撃防御方法、サービス不能攻撃防御装置中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムの好適な実施の形態を詳細に説明する。なお、下記に示す実施例1では、アドレス発行サーバ装置から中継装置に対して正規アドレス情報の送信要求を

おこなう場合を示し、実施例2では正規アドレス情報を一括管理する正規アドレス情報提供サーバへゲート装置から正規アドレス情報の送信要求をおこなう場合を示すこととする。また、実施例3では、ゲート装置が中継装置に対して容疑シグネチャを送信し、その応答として正規アドレス情報を取得する場合を示すこととする。

### 実施例 1

- [0090] 図1は、本実施例1に係る分散型サービス不能攻撃防御システム1の構成を示すブロック図である。同図に示す分散型サービス不能攻撃防御システム1は、通信機器7への分散型サービス不能攻撃を主としてゲート装置8で防御するシステムである。具体的には、ネットワーク2上に所在する正当な装置(アドレス発行サーバ10)により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置8が取得し、取得した正規アドレス情報に基づいてゲート装置8が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器7へ攻撃をおこなうパケットの通過を制限するようにしている。なお、このゲート装置8が正規条件情報に基づいて生成した正規シグネチャ並びに容疑シグネチャは中継装置6などに中継され、中継装置でのフィルタリングを可能ならしめている。
- [0091] 従来、かかる正規アドレス情報の追加や変更等の管理は、ゲート装置8のオペレータによって行われていたため、正規条件情報の管理が煩雑になるという問題があった。このため、本実施例1では、かかる正規アドレス情報の追加をゲート装置8のオペレータに担わせるのではなく、アドレス発行サーバ10などの正当な端末から正規アドレス情報を取得することとしている。このため、本実施例1によれば、ゲート装置8のオペレータの管理負担を軽減することができる。
- [0092] ここで、このゲート装置8が正規アドレス情報を取得する際に、本実施例1では、ゲート装置8が中継装置6に対して自装置のアドレス情報を通知し(図1のステップ1)、この中継装置6にアドレス情報を記憶させ(図1のステップ2)、アドレス発行サーバ10から発行された正規アドレス情報送信要求(正規アドレス情報を含む)を中継装置6が受信すると、あらかじめ記憶したアドレス情報に基づいてゲート装置8に中継し(図1のステップ3)、ゲート装置8が受信した正規アドレス情報に基づいて正規条件情報

を自動生成する(図1のステップ4)こととしている。

[0093] 次に、この分散型サービス不能攻撃防御システム1のシステム構成について説明する。図1に示すように、この分散型サービス不能攻撃防御システム1は、ネットワーク2を介して伝送されるパケットを中継する複数の中継装置3～6と、ネットワーク2を介して通信機器7に送信されるパケットの通過を制限するゲート装置8とを備えている。なお、図1に示した分散型サービス不能攻撃防御システム1の構成は一例を示すものであり、中継装置およびゲート装置等の数量やネットワーク構成を限定するものではない。

[0094] ゲート装置8は、ネットワーク間接続機器であるゲートウェイ装置などによって構成され、コンピュータ装置等によって構成される通信機器7を含む構内情報通信網(Local Area Network、以下単に「LAN」と記載する。)14に接続されている。また、中継装置3～6は、ルータ装置によってそれぞれ構成されている。なお、この中継装置3～6は、ブリッジによって構成することもできる。

[0095] ここで、中継装置3は、中継装置4およびゲート装置8に接続され、中継装置4は、通信機器15および中継装置3に接続され、中継装置5は、通信機器16および中継装置6に接続され、中継装置6は、中継装置5、エッジルータ11およびゲート装置8に接続されている。

[0096] 図2は、図1に示したゲート装置8の構成を示すブロック図である。図2に示すように、このゲート装置8は、ネットワーク2から受信されたパケットによる攻撃を検知する攻撃検知部20と、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成部21と、通信機器7に対する攻撃とみなされないパケット(非攻撃パケット)の条件を表す正規条件情報を格納する正規条件情報格納部22と、正規条件情報格納部22に格納される正規条件情報を生成する正規条件情報生成部23と、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成部24と、容疑シグネチャに当てはまるパケットのうち、通信機器7に対する攻撃とみなすパケットの特徴を表す不正シグネチャを生成する不正シグネチャ生成部25と、容疑シグネチャ、正規シグネチャおよび不正シグネチャに基づいてネットワーク2から受信されたパケ

ットの通過を制限するパケット制限部26と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に通知するシグネチャ通知部27と、ネットワーク2に接続された各装置と通信を行うネットワークインタフェース28とを備えている。

- [0097] 攻撃検知部20は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図3は、攻撃検知条件の一例を示す図である。図3において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる3組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。
- [0098] 例えば、1番目の検知条件は、宛先のアドレス情報が192.168.1.1であり(Dst=192.168.1.1/32)、トランスポート層のプロトコルがTCP(TransmissionControlProtocol)であり(Protocol=TCP)、TCPポート番号が80である(Port=80)パケットが検知対象となり、この検知対象のパケットの伝送レートが500kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
- [0099] 同様に、2番目の検知条件は、宛先のアドレス情報が192.168.1.2であり(Dst=192.168.1.2/32)、トランスポート層のプロトコルがUDP(Userdatagramprotocol)である(Protocol=UDP)パケットが検知対象となり、この検知対象のパケットの伝送レートが300kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
- [0100] また、3番目の検知条件は、宛先のアドレス情報が192.168.1.0~192.168.1.255の範囲内である(Dst=192.168.1.0/24)パケットが検知対象となり、この検知対象のパケットの伝送レートが1Mbpsを超えた状態が20秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
- [0101] このように、検知対象のパケットによる攻撃が攻撃検知部20によって検知されると、容疑シグネチャ生成部21は、検知対象のパケットの特徴を表す容疑シグネチャを生成する。例えば、図3における攻撃検知条件の1番目の検知条件に合う攻撃が検知された場合には、容疑シグネチャ生成部21は、宛先のアドレス情報が192.168.1.1で

あり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であるパケットを示す容疑シグネチャを生成する。なお、容疑シグネチャは、対象となるパケットに対するシェーピングやフィルタリング等の処理や、この処理に関するパラメータ等を含むようにしてもよい。

- [0102] 正規条件情報格納部22は、フラッシュメモリなどの不揮発性の記憶媒体によって構成されている。図4は、正規条件情報格納部22に格納される正規条件情報の一例を示す図である。図4において、正規条件情報は攻撃とみなされない条件である正規条件で構成される。
- [0103] 例えば、1番目の正規条件によって、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内である(Src=172.16.10.0/24)パケットは、攻撃とみなされない。同様に、2番目の正規条件によって、サービスタイプ(TypeofService)が0x01である(TOS=0x01)パケットは、攻撃とみなされない。
- [0104] 正規条件情報生成部23は、本実施例1の最も重要な特徴部分をなす処理部であり、オペレータの処理行為を伴うことなく正規条件情報格納部22に格納された正規条件情報の自動更新をおこなう。従来、かかる正規条件情報の管理はオペレータに委ねられていたが、本実施例1では、かかる正規条件情報を自動更新している。
- [0105] 具体的には、この正規条件情報生成部23は、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報が何れかの中継装置3～6から送信され、送信された正規アドレス情報がネットワークインタフェース28に受信された場合に、正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部22に格納された正規条件情報を更新する。すなわち、正規アドレス情報を送信アドレスとしたパケットは、通信機器7に対する攻撃とみなされないものとなる。なお、ここでは正規条件情報の追加を自動的におこなう点を強調したが、正規条件情報格納部22に格納された正規条件情報は、ゲート装置8のオペレータによって追加、削除、変更などの編集ができるようにしてもよい。
- [0106] 正規シグネチャ生成部24は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する処理部である。

- [0107] 例えば、この正規シグネチャ生成部24は、攻撃検知部20によって図3に示した1番目の攻撃検知条件に合う攻撃が検知された場合には、図4に示した正規条件情報に基づいて、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内であるパケットを示す正規シグネチャと、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、サービスタイプが0x01であるパケットを示す正規シグネチャとを生成する。
- [0108] 不正シグネチャ生成部25は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャを生成する処理部である。
- [0109] 図5は、不正条件の一例を示す図である。図5において、1番目の不正条件は、500 kbps以上の伝送レートで30秒以上連続送信されているパケットを示している。同様に、2番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されているICMP (Internet Control Message Protocol) に準拠したエコー応答 (Echo Reply) パケットを示し、3番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されている分割送信されたフラグメントパケットを示している。
- [0110] パケット制限部26は、容疑シグネチャ生成部21によって生成された容疑シグネチャと正規シグネチャ生成部24によって生成された正規シグネチャと不正シグネチャ生成部25によって生成された不正シグネチャに基づいてネットワークインタフェース28によって受信されたパケットの通過を制限するようになっている。
- [0111] 具体的には、パケット制限部26は、不正シグネチャに当てはまるパケットを廃棄し、正規シグネチャに当てはまるパケットに対しては制限を加えずに通過させ、容疑シグネチャに当てはまるパケットに対しては容疑シグネチャに示された処理等に基づいて伝送帯域を絞った経路を介して通過させるようになっている。
- [0112] シグネチャ通知部27は、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に通知する処理部であり、中継装置3および中継装置6は、さらに隣接関係にある中継装置にパケットを中継する。なお、隣接関係とは、本発明に係るゲート装置および中継装置における隣接関係であり、物理的な接続関係

とは異なる。

- [0113] また、シグネチャ通知部27は、ゲート装置8のアドレス情報を容疑シグネチャおよび正規シグネチャと同様に隣接関係にある中継装置3および中継装置6に通知し、中継装置3および中継装置6は、さらに隣接関係にある中継装置にゲート装置8のアドレス情報を中継する。なお、シグネチャ通知部27によるゲート装置8のアドレス情報の通知は、ゲート装置8のオペレータによる起動に応じて行なうことができ、定期的に行われるようにしてもよい。
- [0114] 図6は、図1に示した中継装置6の構成を示す機能ブロック図である。なお、ここでは説明の便宜上中継装置6の構成を説明するが、他の中継装置3～5についても中継装置6と同様に構成されている。この中継装置6は、入力ポート30と、パケットをルーティングするためのスイッチ31と、出力ポート32と、不正シグネチャを生成する不正シグネチャ生成部35と、不正シグネチャならびにゲート装置8によって通知された容疑シグネチャおよび正規シグネチャに基づいて入力ポート30に入力されたパケットの通過を制限するパケット制限部36と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置5に中継するシグネチャ中継部37と、ゲート装置8のアドレス情報を記憶するアドレス情報記憶部38と、アドレス情報記憶部38に記憶されたゲート装置8のアドレス情報に基づいて正規アドレス情報を送信する正規アドレス情報送信部39とを備えている。
- [0115] ここで、不正シグネチャ生成部35、パケット制限部36およびシグネチャ中継部37は、ゲート装置8を構成する不正シグネチャ生成部25、パケット制限部26およびシグネチャ通知部27とそれぞれ同様に構成されるため、詳細な説明は省略する。なお、中継装置6は、ゲート装置8と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部および正規シグネチャ生成部を備えるようにしてもよい。
- [0116] シグネチャ中継部37は、パケット制限部36によってパケットの通過が制限された後、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート30に受信されているか否かを判断し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート30に受信されていると判断した場合には、容疑シグネチャおよび正規シグネチャを中継し、制限された伝送レートを超えた容疑シグネ

チャに当てはまるパケットが入力ポート30に受信されていると判断しなかった場合には、容疑シグネチャおよび正規シグネチャを中継しない。

[0117] また、図1に示した構成においては、中継装置4および中継装置5には、容疑シグネチャおよび正規シグネチャを中継する中継装置が存在しないため、シグネチャ中継部37による容疑シグネチャおよび正規シグネチャの中継は行われない。

[0118] このように、ゲート装置8によって攻撃が検知された場合には、容疑シグネチャおよび正規シグネチャが生成され、生成された容疑シグネチャおよび正規シグネチャが各中継装置3～6に通知され、ゲート装置8および中継装置3～6においてパケットのシェーピングやフィルタリング等の処理が施される。このため、分散型サービス不能攻撃防御システム1においては、例えば、ゲート装置8によって検知された攻撃が通信機器15を介して行われている場合には、攻撃を行うパケットの通過が攻撃元の近く、すなわち中継装置4で制限され、攻撃を行うパケットによる悪影響が小さくなる。

[0119] アドレス情報記憶部38は、不揮発性の記憶媒体によって構成されており、ゲート装置8のシグネチャ通知部27や各中継装置のシグネチャ中継部37を介して通知および中継されたゲート装置8のアドレス情報を記憶する。なお、図1においては、一つゲート装置8を図示しているが、本実施例1の分散型サービス不能攻撃防御システム1は、複数のゲート装置によって構成することもでき、この場合にアドレス情報記憶部38には、各ゲート装置のアドレス情報が記憶されることになる。

[0120] 図1において、LAN9は、エッジルータ11を介してネットワーク2と接続されるとともに、コンピュータ装置等の通信機器12、13が接続されている。ここで、LAN9では、ネットワーク2を介した攻撃を行わないものとする。

[0121] LAN9に接続されたアドレス発行サーバ10は、LAN9のアドレス情報またはLAN9に接続された通信機器12、13のアドレス情報を含む正規アドレス情報送信要求を中継装置6に向けて送信する。なお、このアドレス発行サーバ10は、正規アドレス情報送信要求を定期的に送信するようにしてもよく、アドレス発行サーバ10のオペレータによる起動に応じて送信するようにしてもよい。また、正規アドレス情報送信要求を送信するものとしては、アドレス発行サーバ10の他にエッジルータ11等のLAN9を構成する装置であれば何れのものでもよい。

- [0122] 図6において、正規アドレス情報送信部39は、アドレス発行サーバ10によって送信された正規アドレス情報送信要求に応答して、正規アドレス情報送信要求に含まれるアドレス情報、すなわち正規アドレス情報をアドレス情報記憶部38に記憶された各ゲート装置のアドレス情報に基づいて送信する。
- [0123] 以上のように構成された分散型サービス不能攻撃防御システム1について、図7～図10を用いてその動作を説明する。図7は、図1に示したゲート装置8の攻撃検知動作を示すフローチャートである。
- [0124] まず、攻撃検知条件に基づいてネットワークインタフェース28によって受信されたパケットによる攻撃が攻撃検知部20によって検知されると(ステップS1)、攻撃が検知されたパケットの特徴を表す容疑シグネチャが容疑シグネチャ生成部21によって生成される(ステップS2)。
- [0125] 次に、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャが正規シグネチャ生成部24によって生成されるとともに(ステップS3)、容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部25によって生成される(ステップS4)。
- [0126] 次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部26によるパケット通過条件として設定される(ステップS5)。また、容疑シグネチャおよび正規シグネチャがシグネチャ通知部27によって隣接関係にある中継装置3および中継装置6に通知される(ステップS6)。
- [0127] 図8は、図1に示した中継装置6のシグネチャ受信動作を示すフローチャートである。まず、入力ポート30に容疑シグネチャおよび正規シグネチャが受信されると(ステップS10)、受信された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部35によって生成される(ステップS11)。
- [0128] 次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部36によるパケット通過条件として設定される(ステップS12)。また、容疑シグネチャおよび正規シグネチャがシグネチャ中継部37によって隣接関係にある中継装置5に通知

される(ステップS13)。

- [0129] 図9は、図1に示したゲート装置8の packets 制限動作を示すフローチャートである。まず、ネットワークインタフェース28に packets が受信されると(ステップS20)、受信された packets が不正シグネチャに当てはまるか否かが packets 制限部26によって判断される(ステップS21)。
- [0130] packets が不正シグネチャに当てはまると判断された場合には、packets が packets 制限部26によって廃棄される(ステップS22)。一方、packets が不正シグネチャに当てはまらなないと判断された場合には、packets が正規シグネチャに当てはまるか否かが packets 制限部26によって判断される(ステップS23)。
- [0131] packets が正規シグネチャに当てはまると判断された場合には、packets の通過が packets 制限部26によって許可される(ステップS24)。一方、packets が正規シグネチャに当てはまらなないと判断された場合には、packets が容疑シグネチャに当てはまるか否かが packets 制限部26によって判断される(ステップS25)。
- [0132] packets が容疑シグネチャに当てはまると判断された場合には、容疑シグネチャに示された処理等に基づいて伝送帯域が絞られた経路を介した packets の通過が許可される(ステップS26)。一方、packets が容疑シグネチャに当てはまらなないと判断された場合には、packets の通過が packets 制限部26によって許可される(ステップS24)。なお、中継装置3～6の packets 制限動作は、ゲート装置8の packets 制限動作と同様であるため説明を省略する。
- [0133] 図10は、分散型サービス不能攻撃防御システム1の正規条件情報更新動作を示すシーケンス図である。まず、ゲート装置8のアドレス情報が、ゲート装置8のシグネチャ通知部27によって中継装置3および中継装置6にそれぞれ通知される(ステップS30、S31)。中継装置3に通知されたゲート装置8のアドレス情報は、中継装置3のシグネチャ中継部37によって中継装置4に中継される(ステップS32)。
- [0134] 中継装置6に通知されたゲート装置8のアドレス情報は、中継装置6のシグネチャ中継部37によって中継装置5に中継されるとともに(ステップS33)、アドレス情報記憶部38に記憶される(ステップS34)。なお、中継装置3～5においてもアドレス情報記憶部38にゲート装置8のアドレス情報が記憶されるがここでは図示省略する。

- [0135] ここで、LAN9のアドレス発行サーバ10によって正規アドレス情報送信要求が中継装置6に送信されると(ステップS35)、中継装置6のアドレス情報記憶部38に記憶されたゲート装置8のアドレス情報に基づいて正規アドレス情報送信要求に含まれる正規アドレス情報が送信される(ステップS36)。
- [0136] 正規アドレス情報がゲート装置8のネットワークインタフェース28に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部23によって生成され(ステップS37)、生成された正規条件情報を以って正規条件情報格納部22に格納された正規条件情報が更新される(ステップS38)。
- [0137] 以上説明したように、分散型サービス不能攻撃防御システム1によれば、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報がゲート装置8に送信され、ゲート装置8に送信された正規アドレス情報に基づいて、通信機器7に対する攻撃とみなされないパケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

## 実施例 2

- [0138] ところで、上記実施例1では、ゲート装置8が正規アドレス情報を取得する際に、本実施例1では、ゲート装置8のアドレス情報を中継装置6で記憶しておき、この中継装置6がアドレス発行サーバ10から発行された正規アドレス情報送信要求(正規アドレス情報を含む)を受信すると、あらかじめ記憶したアドレス情報に基づいてゲート装置8に中継することにより、ゲート装置8が正規アドレス情報を取得することとしたが、本発明はこれに限定されるものではない。そこで、本実施例2では、正規アドレス情報を一括管理する正規アドレス情報提供サーバを設け、この正規アドレス情報提供サーバへの要求に応答してゲート装置が正規アドレス情報を取得する場合を説明する。
- [0139] 図11は、本発明の実施例2に係る分散型サービス不能攻撃防御システム50の構成を示すブロック図である。なお、分散型サービス不能攻撃防御システム50の各構成において実施例1に係る分散型サービス不能攻撃防御システム1の各構成と同様なものについては同一の符号を付して説明を省略する。
- [0140] 同図に示す分散型サービス不能攻撃防御システム50は、正規アドレス情報を一括管理する正規アドレス情報提供サーバ59からゲート装置58に対して正規アドレス情

報を提供している。具体的には、アドレス発行サーバ60があらかじめ正規アドレス情報提供サーバ59に正規アドレス情報を通知し(図11のステップ1)、この正規アドレス情報提供サーバ59に正規アドレス情報を記憶しておく(図11のステップ2)。そして、ゲート装置58から正規アドレス情報提供サーバ59に正規アドレス情報送信要求がなされると(図11のステップ3)、この正規アドレス情報提供サーバ59がゲート装置58に正規アドレス情報を送信し(図11のステップ4)、ゲート装置58が受信した正規アドレス情報に基づいて正規条件情報を自動生成する(図11のステップ5)こととしている。なお、ここでは説明の便宜上、正規アドレス情報提供サーバ59がアドレス発行サーバ60により発行された正規アドレス情報を記憶する場合を示したが、この正規アドレス情報提供サーバ59は、正当な端末である他のアドレス発行サーバや通信機器により発行された正規アドレス情報についても記憶する。たとえば、図中に示す通信機器16が通信機器17等を攻撃するパケットを送出しない正当な装置であると認証されている場合には、正規アドレス情報提供サーバ59は、かかる通信機器16により発行された正規アドレス情報についても記憶する。

[0141] 次に、この分散型サービス不能攻撃防御システム50のシステム構成について説明する。図11に示すように、分散型サービス不能攻撃防御システム50は、ネットワーク2を介して伝送されるパケットを中継する複数の中継装置53～56と、ネットワーク2を介して通信機器7に送信されるパケットの通過を制限するゲート装置58と、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報を記憶する正規アドレス情報記憶装置59とを備えている。なお、図11に示した分散型サービス不能攻撃防御システム50の構成は、一例を示すものであり、中継装置、およびゲート装置等の数量やネットワーク構成を限定するものではない。

[0142] ゲート装置58は、ゲートウェイ装置によって構成され、LAN14に接続されている。また、中継装置53～56は、ルータ装置によってそれぞれ構成されている。なお、中継装置53～56は、ブリッジによってそれぞれ構成されていてもよい。

[0143] ここで、中継装置53は、中継装置54およびゲート装置58に接続され、中継装置54は、通信機器15、中継装置53および正規アドレス情報記憶装置59に接続され、中継装置55は、通信機器16および中継装置56に接続され、中継装置56は、中継

装置55、エッジルータ11およびゲート装置58に接続されているものとする。

[0144] 図12は、図11に示したゲート装置58の構成を示すブロック図である。このゲート装置58は、攻撃検知部20と、容疑シグネチャ生成部21と、正規条件情報格納部22と、正規条件情報格納部22に格納される正規条件情報を生成する正規条件情報生成部73と、正規シグネチャ生成部24と、不正シグネチャ生成部25と、パケット制限部26と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に通知するシグネチャ通知部77と、ネットワークインタフェース28とを備えている。

[0145] 正規条件情報生成部73は、正規アドレス情報の送信を要求する正規アドレス情報送信要求を正規アドレス情報記憶装置59に送信する。正規条件情報生成部73は、正規アドレス情報送信要求に応じて正規アドレス情報記憶装置59によって送信された正規アドレス情報がネットワークインタフェース28に受信された場合に、正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以て正規条件情報格納部22に格納された正規条件情報を更新する。なお、正規条件情報生成部73による正規アドレス情報送信要求の送信は、ゲート装置58のオペレータによる起動に応じて行われるようにしてもよく、定期的に行われるようにしてもよい。シグネチャ通知部77は、上記実施例1において説明したゲート装置8を構成するシグネチャ通知部27に対してゲート装置のアドレス情報の通知を行わない点が相違する。

[0146] 図13は、図11に示した中継装置56のブロック図である。なお、ここでは説明の便宜上中継装置56の構成を説明するが、中継装置53～55についても中継装置56と同様に構成されている。中継装置56は、入力ポート30と、スイッチ31と、出力ポート32と、不正シグネチャ生成部35と、パケット制限部36と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置5に中継するシグネチャ中継部87とを備えている。

[0147] ここで、シグネチャ中継部87は、ゲート装置58を構成するシグネチャ通知部77と同様に構成されるため、詳細な説明は省略する。なお、中継装置56は、ゲート装置58と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部、および正規シグネチャ生成部を備えるようにしてもよい。

- [0148] 図11において、LAN9に接続されたアドレス発行サーバ60は、LAN9のアドレス情報、またはLAN9に接続された通信機器12、13のアドレス情報、すなわち正規アドレス情報を正規アドレス情報記憶装置59に登録する。
- [0149] なお、アドレス発行サーバ60は、正規アドレス情報を定期的に登録するようにしてもよく、アドレス発行サーバ60のオペレータによる起動に応じて登録するようにしてもよい。また、正規アドレス情報を登録するものとしては、アドレス発行サーバ60の他にエッジルータ11等のLAN9を構成する装置であれば何れのものでもよい。
- [0150] 以上のように構成された分散型サービス不能攻撃防御システム50について、図14を用いてその動作を説明する。なお、ゲート装置58の攻撃検知動作、中継装置53～56のシグネチャ受信動作、ゲート装置58の packets 制限動作については、実施例1において図7～図9を参照して説明したものと同様であるため説明を省略する。
- [0151] 図14は、本実施例2に係る分散型サービス不能攻撃防御システム50の正規条件情報更新動作を示すシーケンス図である。まず、アドレス発行サーバ60から送信された正規アドレス情報が正規アドレス情報提供サーバ59に格納される(ステップS41)。ゲート装置58の正規条件情報生成部73によって正規アドレス情報送信要求が正規アドレス情報記憶装置59に向けて送信されると(ステップS42)、正規アドレス情報送信要求に応答して正規アドレス情報記憶装置59から正規アドレス情報がゲート装置58に向けて送信される(ステップS43)。
- [0152] 正規アドレス情報がゲート装置58のネットワークインタフェース28に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部73によって生成され(ステップS44)、生成された正規条件情報を以って正規条件情報格納部22に格納された正規条件情報が更新される(ステップS45)。
- [0153] 以上説明したように、分散型サービス不能攻撃防御システム50によれば、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報がゲート装置58からの要求に応じて送信され、ゲート装置58に送信された正規アドレス情報に基づいて、通信機器7に対する攻撃とみなされないパケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。
- [0154] なお、上記実施例1および2に示したゲート装置は、コンピュータにプログラムをロー

ドして実行することにより機能発揮する。具体的には、コンピュータのROM(ReadOnlyMemory)等に正規アドレス情報を取得するルーチン、正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成するルーチン、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するルーチンを含むプログラムを記憶しておき、かかるプログラムをCPUにロードして実行することにより、本発明に係るゲート装置を形成することができる。

### 実施例 3

- [0155] 実施例3では、ゲート装置が中継装置に対して容疑シグネチャを送信し、その応答として正規アドレス情報を取得する場合について説明する。図15は、本実施例3に係る分散型サービス不能攻撃防御システム101の構成を示すブロック図である。同図に示す分散型サービス不能攻撃防御システム101は、通信機器107への分散型サービス不能攻撃を主としてゲート装置108で防御するシステムである。具体的には、ネットワーク102上に所在する正当な装置(アドレス発行サーバ110)により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置108が取得し、取得した正規アドレス情報に基づいてゲート装置108が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器107へ攻撃をおこなうパケットの通過を制限するようにしている。なお、このゲート装置108が正規条件情報に基づいて生成した正規シグネチャ並びに容疑シグネチャは中継装置106などに転送され、中継装置でのフィルタリングを可能ならしめている。
- [0156] 従来、かかる正規アドレス情報の追加や変更等の管理は、ゲート装置108のオペレータによって行われていたため、正規条件情報の管理が煩雑になるという問題があった。このため、本実施例3では、かかる正規アドレス情報の追加をゲート装置108のオペレータに担わせるのではなく、アドレス発行サーバ110などの正当な端末から正規アドレス情報を取得することとしている。このため、本実施例3によれば、ゲート装置108のオペレータの管理負担を軽減することができる。
- [0157] ここで、このゲート装置108が正規アドレス情報を取得する際に、本実施例3では、

アドレス発行サーバ110が中継装置106に対して正規アドレス情報を送信し(図15のステップ1)、この中継装置106に正規アドレス情報を記憶させ(図15のステップ2)、ゲート装置108が攻撃を検知したパケットの特徴を表す容疑シグネチャを生成して生成した容疑シグネチャを中継装置106に送信すると(図15のステップ3)、あらかじめ記憶した正規アドレス情報をゲート装置108に転送し(図15のステップ4)、ゲート装置108が正規アドレス情報に基づいて正規条件情報を自動生成する(図15のステップ5)こととしている。

[0158] 次に、この分散型サービス不能攻撃防御システム101のシステム構成について説明する。図15に示すように、この分散型サービス不能攻撃防御システム101は、ネットワーク102を介して伝送されるパケットを中継する複数の中継装置103～106と、ネットワーク102を介して通信機器107に送信されるパケットの通過を制限するゲート装置108とを備えている。なお、図15に示した分散型サービス不能攻撃防御システム101の構成は一例を示すものであり、中継装置およびゲート装置等の数量やネットワーク構成を限定するものではない。

[0159] ゲート装置108は、ネットワーク間接続機器であるゲートウェイ装置などによって構成され、コンピュータ装置等によって構成される通信機器107を含む構内情報通信網(LocalAreaNetwork、以下単に「LAN」と記載する。)114に接続されている。また、中継装置103～106は、ルータ装置によってそれぞれ構成されている。なお、この中継装置103～106は、ブリッジによって構成することもできる。

[0160] ここで、中継装置103は、中継装置104およびゲート装置108に接続され、中継装置104は、通信機器115および中継装置103に接続され、中継装置105は、通信機器116および中継装置106に接続され、中継装置106は、中継装置105、エッジルータ111およびゲート装置108に接続されている。

[0161] 図16は、図15に示したゲート装置108の構成を示すブロック図である。図16に示すように、このゲート装置108は、ネットワーク102から受信されたパケットによる攻撃を検知する攻撃検知部120と、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成部121と、通信機器107に対する攻撃とみなされないパケット(非攻撃パケット)の条件を表す正規条件情報を格納する正規条件情

報格納部122と、正規条件情報格納部122に格納される正規条件情報を生成する正規条件情報生成部123と、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成部124と、容疑シグネチャに当てはまるパケットのうち、通信機器107に対する攻撃とみなすパケットの特徴を表す不正シグネチャを生成する不正シグネチャ生成部125と、容疑シグネチャ、正規シグネチャおよび不正シグネチャに基づいてネットワーク102から受信されたパケットの通過を制限するパケット制限部126と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置103および中継装置106に転送するシグネチャ転送部127と、ネットワーク102に接続された各装置と通信を行うネットワークインタフェース128とを備えている。

- [0162] 攻撃検知部120は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図17は、攻撃検知条件の一例を示す図である。図17において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる3組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。
- [0163] 例えば、1番目の検知条件は、宛先のアドレス情報が192.168.1.1であり(Dst=192.168.1.1/32)、トランスポート層のプロトコルがTCP(TransmissionControlProtocol)であり(Protocol=TCP)、TCPポート番号が80である(Port=80)パケットが検知対象となり、この検知対象のパケットの伝送レートが500kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
- [0164] 同様に、2番目の検知条件は、宛先のアドレス情報が192.168.1.2であり(Dst=192.168.1.2/32)、トランスポート層のプロトコルがUDP(Userdatagramprotocol)である(Protocol=UDP)パケットが検知対象となり、この検知対象のパケットの伝送レートが300kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
- [0165] また、3番目の検知条件は、宛先のアドレス情報が192.168.1.0～192.168.1.255の範囲内である(Dst=192.168.1.0/24)パケットが検知対象となり、この検知対象のパケ

ットの伝送レートが1Mbpsを超えた状態が20秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

- [0166] このように、検知対象のパケットによる攻撃が攻撃検知部120によって検知されると、容疑シグネチャ生成部121は、検知対象のパケットの特徴を表す容疑シグネチャを生成する。例えば、図17における攻撃検知条件の1番目の検知条件に合う攻撃が検知された場合には、容疑シグネチャ生成部121は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であるパケットを示す容疑シグネチャを生成する。なお、容疑シグネチャは、対象となるパケットに対するシェーピングやフィルタリング等の処理や、この処理に関するパラメータ等を含むようにしてもよい。
- [0167] 正規条件情報格納部122は、フラッシュメモリなどの不揮発性の記憶媒体によって構成されている。図18は、正規条件情報格納部122に格納される正規条件情報の一例を示す図である。図18において、正規条件情報は攻撃とみなされない条件である正規条件で構成される。
- [0168] 例えば、1番目の正規条件によって、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内である(Src=172.16.10.0/24)パケットは、攻撃とみなされない。同様に、2番目の正規条件によって、サービスタイプ(TypeofService)が0x01である(TOS=0x01)パケットは、攻撃とみなされない。
- [0169] 正規条件情報生成部123は、本実施例3の最も重要な特徴部分をなす処理部であり、オペレータの処理行為を伴うことなく正規条件情報格納部122に格納された正規条件情報の自動更新をおこなう。従来、かかる正規条件情報の管理はオペレータに委ねられていたが、本実施例3では、かかる正規条件情報を自動更新している。
- [0170] 具体的には、この正規条件情報生成部123は、ネットワーク102を介した攻撃を行わないパケットの送信元を表す正規アドレス情報が隣接する中継装置103または106から送信され、送信された正規アドレス情報がネットワークインタフェース128に受信された場合に、この正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部122に格納された正規条件情報を更新する。すなわち、正規アドレス情報を送信アドレスとしたパケットは、通信機器107に

対する攻撃とみなされないものとなる。なお、ここでは正規条件情報の追加を自動的に起こう点を強調したが、正規条件情報格納部122に格納された正規条件情報は、ゲート装置108のオペレータによって追加、削除、変更などの編集ができるようにしてもよい。

[0171] 正規シグネチャ生成部124は、容疑シグネチャ生成部121によって生成された容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する処理部である。

[0172] 例えば、この正規シグネチャ生成部124は、攻撃検知部120によって図17に示した1番目の攻撃検知条件に合う攻撃が検知された場合には、図18に示した正規条件情報に基づいて、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内であるパケットを示す正規シグネチャと、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、サービスタイプが0x01であるパケットを示す正規シグネチャとを生成する。

[0173] 不正シグネチャ生成部125は、容疑シグネチャ生成部121によって生成された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャを生成する処理部である。

[0174] 図19は、不正条件の一例を示す図である。図19において、1番目の不正条件は、500kbps以上の伝送レートで30秒以上連続送信されているパケットを示している。同様に、2番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されているICMP (InternetControlMessageProtocol) に準拠したエコー応答 (EchoReply) パケットを示し、3番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されている分割送信されたフラグメントパケットを示している。

[0175] パケット制限部126は、容疑シグネチャ生成部121によって生成された容疑シグネチャと正規シグネチャ生成部124によって生成された正規シグネチャと不正シグネチャ生成部125によって生成された不正シグネチャに基づいてネットワークインタフェース128によって受信されたパケットの通過を制限するようになっている。

- [0176] 具体的には、パケット制限部126は、不正シグネチャに当てはまるパケットを廃棄し、正規シグネチャに当てはまるパケットに対しては制限を加えずに通過させ、容疑シグネチャに当てはまるパケットに対しては容疑シグネチャに示された処理等に基づいて伝送帯域を絞った経路を介して通過させるようになっている。
- [0177] シグネチャ転送部127は、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置103および中継装置106に転送する処理部であり、中継装置103および中継装置106は、さらに隣接関係にある中継装置にパケットを転送する。なお、隣接関係とは、本発明に係るゲート装置および中継装置における隣接関係であり、物理的な接続関係とは異なる。
- [0178] 図20は、図15に示した中継装置106の構成を示す機能ブロック図である。なお、ここでは説明の便宜上中継装置106の構成を説明するが、他の中継装置103～105についても中継装置106と同様に構成されている。この中継装置106は、入力ポート130と、パケットをルーティングするためのスイッチ131と、出力ポート132と、不正シグネチャを生成する不正シグネチャ生成部135と、不正シグネチャならびにゲート装置108によって転送された容疑シグネチャおよび正規シグネチャに基づいて入力ポート130に入力されたパケットの通過を制限するパケット制限部136と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置105に転送するシグネチャ転送部137と、中継装置106の保持する正規アドレス情報を格納する正規アドレス情報格納部138と、正規アドレス情報格納部138に格納された正規アドレス情報を送信する正規アドレス情報送信部139を備えている。
- [0179] ここで、不正シグネチャ生成部135、パケット制限部136およびシグネチャ転送部137は、ゲート装置108を構成する不正シグネチャ生成部125、パケット制限部126およびシグネチャ転送部127とそれぞれ同様に構成されるため、詳細な説明は省略する。なお、中継装置106は、ゲート装置108と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部および正規シグネチャ生成部を備えるようにしてもよい。
- [0180] シグネチャ転送部137は、パケット制限部136によってパケットの通過が制限された後、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート

130に受信されているか否かを判断し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート130に受信されていると判断した場合には、容疑シグネチャおよび正規シグネチャを転送し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート130に受信されていると判断しなかった場合には、容疑シグネチャおよび正規シグネチャを転送しない。

[0181] また、図15に示した構成においては、中継装置104および中継装置105には、容疑シグネチャおよび正規シグネチャを転送する中継装置が存在しないため、シグネチャ転送部137による容疑シグネチャおよび正規シグネチャの転送は行われない。

[0182] このように、ゲート装置108によって攻撃が検知された場合には、容疑シグネチャおよび正規シグネチャが生成され、生成された容疑シグネチャおよび正規シグネチャが各中継装置103～106に転送され、ゲート装置108および中継装置103～106においてパケットのシェーピングやフィルタリング等の処理が施される。このため、分散型サービス不能攻撃防御システム101においては、例えば、ゲート装置108によって検知された攻撃が通信機器115を介して行われている場合には、攻撃を行うパケットの通過が攻撃元の近く、すなわち中継装置104で制限され、攻撃を行うパケットによる悪影響が小さくなる。

[0183] アドレス情報格納部138は、不揮発性の記憶媒体によって構成されており、正規アドレス情報を保持する。

[0184] 図15において、LAN109は、エッジルータ111を介してネットワーク102と接続されるとともに、コンピュータ装置等の通信機器112、113が接続されている。ここで、LAN109では、ネットワーク102を介した攻撃を行わないものとする。

[0185] LAN109に接続されたアドレス発行サーバ110は、LAN109のアドレス情報またはLAN109に接続された通信機器112、113のアドレス情報を含む正規アドレス情報を中継装置106に向けて送信する。なお、このアドレス発行サーバ110は、正規アドレス情報を定期的に送信するようにしてもよく、アドレス発行サーバ110のオペレータによる起動に応じて送信するようにしてもよい。また、正規アドレス情報を送信するものとしては、アドレス発行サーバ110の他にエッジルータ111等のLAN109を構成する装置であれば何れのものでもよい。

- [0186] 図20において、正規アドレス情報格納部138はさらに、アドレス発行サーバ110によって送信された正規アドレス情報を正規アドレス情報格納部138に追加するようになっている。
- [0187] 以上のように構成された分散型サービス不能攻撃防御システム101について、図21～図24を用いてその動作を説明する。図21は、図15に示したゲート装置108の攻撃検知動作を示すフローチャートである。
- [0188] まず、攻撃検知条件に基づいてネットワークインタフェース128によって受信されたパケットによる攻撃が攻撃検知部120によって検知されると(ステップS101)、攻撃が検知されたパケットの特徴を表す容疑シグネチャが容疑シグネチャ生成部121によって生成される(ステップS102)。
- [0189] 次に、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャが正規シグネチャ生成部124によって生成されるとともに(ステップS103)、容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部125によって生成される(ステップS104)。
- [0190] 次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部126によるパケット通過条件として設定される(ステップS105)。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部127によって隣接関係にある中継装置103および中継装置106に転送される(ステップS106)。
- [0191] 図22は、図15に示した中継装置106のシグネチャ受信動作を示すフローチャートである。まず、入力ポート130に容疑シグネチャおよび正規シグネチャが受信されると(ステップS110)、受信された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部135によって生成される(ステップS111)。
- [0192] 次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部136によるパケット通過条件として設定される(ステップS112)。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部137によって隣接関係にある中継装置105に転送される(ステップS113)。さらに正規アドレス情報格納部138に保持している

正規アドレス情報を容疑シグネチャの送信元であるゲート装置108に送信する(ステップS114)。

- [0193] 図23は、図15に示したゲート装置108の packets 制限動作を示すフローチャートである。まず、ネットワークインタフェース128に packets が受信されると(ステップS120)、受信された packets が不正シグネチャに当てはまるか否かが packets 制限部126によって判断される(ステップS121)。
- [0194] packets が不正シグネチャに当てはまると判断された場合には、packets が packets 制限部126によって廃棄される(ステップS122)、一方、packets が不正シグネチャに当てはまらなると判断された場合には、packets が正規シグネチャに当てはまるか否かが packets 制限部126によって判断される(ステップS123)。
- [0195] packets が正規シグネチャに当てはまると判断された場合には、packets の通過が packets 制限部126によって許可される(ステップS124)。一方、packets が正規シグネチャに当てはまらなると判断された場合には、packets が容疑シグネチャに当てはまるか否かが packets 制限部126によって判断される(ステップS125)。
- [0196] packets が容疑シグネチャに当てはまると判断された場合には、容疑シグネチャに示された処理等に基づいて伝送帯域が絞られた経路を介した packets の通過が許可される(ステップS126)。一方、packets が容疑シグネチャに当てはまらなると判断された場合には、packets の通過が packets 制限部126によって許可される(ステップS124)。なお、中継装置103～106の packets 制限動作は、ゲート装置108の packets 制限動作と同様であるため説明を省略する。
- [0197] 図24は、分散型サービス不能攻撃防御システム101の正規条件情報更新動作を示すシーケンス図である。まず、LAN109のアドレス発行サーバ110からLAN109内の正規アドレス情報が中継装置106に送信され(ステップS130)、中継装置106の正規アドレス情報格納部138に格納されるとともに(ステップS131)、通信装置116からの正規アドレス情報が中継装置105に送信され(ステップS132)、中継装置105の正規アドレス情報格納部138に格納される(ステップS133)。
- [0198] ここでゲート装置108において攻撃を検知すると(ステップS134)、対応する容疑シグネチャが生成され(ステップS135)、隣接する中継装置103および中継装置106

に転送される(ステップS136)。以下では、簡単のため中継装置103および中継装置104へのシグネチャの転送については記述を省略する。

- [0199] 中継装置106はゲート装置108から容疑シグネチャを受信すると、正規アドレス情報格納部138に格納してある正規アドレス情報をゲート装置108に送り返し(ステップS137)、容疑シグネチャをさらに中継装置105に転送する(ステップS141)。ここで、ステップS137とステップS141は順序を逆にすることが可能である。
- [0200] 正規アドレス情報がゲート装置108のネットワークインタフェース128に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部123によって生成され、生成された正規条件情報を以って正規条件情報格納部122に格納された正規条件情報が更新される(ステップS138)。次いで、正規シグネチャ生成部124にて、対応する正規シグネチャが生成され、パケット制限と中継装置106への転送が行なわれる(ステップS139～S140)。
- [0201] 一方、中継装置105は、中継装置106から容疑シグネチャを受信すると、正規アドレス情報格納部138に格納してある正規アドレス情報を容疑シグネチャの送信元である中継装置、すなわち中継装置106に送信する(ステップS142)。中継装置106は、中継装置105から受信した正規アドレス情報をそのままゲート装置108に送信する(ステップS143)。
- [0202] 正規アドレス情報がゲート装置108のネットワークインタフェース128に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部123によって生成され、生成された正規条件情報を以って正規条件情報格納部122に格納された正規条件情報が更新される(ステップS144)。次いで、正規シグネチャ生成部124にて、対応する正規シグネチャが生成され、パケット制限と中継装置106への転送が行なわれる(ステップS145～S146)。
- [0203] 以上説明したように、分散型サービス不能攻撃防御システム101によれば、ネットワーク102を介した攻撃を行わないパケットの送信元を表す正規アドレス情報がゲート装置108に送信され、ゲート装置108に送信された正規アドレス情報に基づいて、通信機器107に対する攻撃とみなされないパケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

- [0204] なお、上記実施例3に示したゲート装置108は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、コンピュータのROM (ReadOnlyMemory) 等に容疑シグネチャを送信して正規アドレス情報を取得するルーチン、正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成するルーチン、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するルーチンを含むプログラムを記憶しておき、かかるプログラムをCPUにロードして実行することにより、本発明に係るゲート装置108を形成することができる。

#### 産業上の利用可能性

- [0205] 以上のように、本発明にかかるサービス不能攻撃防御方法、サービス不能攻撃防御システム、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムは、サービス不能攻撃および分散型サービス不能攻撃から通信機器を防御する場合に適している。

### 請求の範囲

- [1] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、
- 前記ネットワーク上に所在する正当な装置が非攻撃パケットの送信元を示す正規アドレス情報を発行し、前記ゲート装置が前記正当な装置が発行した正規アドレス情報に基づいて前記通信機器へ攻撃をおこなうパケットの通過を制限することを特徴とするサービス不能攻撃防御方法。
- [2] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、
- 前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が取得する正規アドレス情報取得工程と、
- 前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて前記ゲート装置が非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、
- 前記ゲート装置が前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程と
- を含んだことを特徴とする請求項1に記載のサービス不能攻撃防御方法。
- [3] 前記正規アドレス情報取得工程は、前記ゲート装置が前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知工程と、前記中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記アドレス情報通知工程により通知された前記アドレス情報に基づいて当該正規アドレス情報を前記ゲート装置に対して中継する正規アドレス情報中継工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする請求項2に記載のサービス不能攻

撃防御方法。

- [4] 前記アドレス情報通知工程は、前記ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置に前記ゲート装置のアドレス情報を中継し、前記正規アドレス情報中継工程は、前記他の中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記ゲート装置のアドレス情報に基づいて隣接する中継装置若しくは前記ゲート装置に前記正規アドレス情報を中継することを特徴とする請求項3に記載のサービス不能攻撃防御方法。
- [5] 前記正規アドレス情報取得工程は、正規アドレス情報を一括管理する正規アドレス情報提供装置が前記正規アドレス情報を各正当な装置から受信して格納する正規アドレス情報格納工程と、前記正規アドレス情報提供装置が前記ゲート装置から前記正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報を前記ゲート装置に対して通知する正規アドレス情報通知工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする請求項2に記載のサービス不能攻撃防御方法。
- [6] 前記正規アドレス情報取得工程は、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器により送信された前記正規アドレス情報を前記ゲート装置が取得することを特徴とする請求項2～5のいずれか一つに記載のサービス不能攻撃防御方法。
- [7] 前記ゲート装置が前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知工程と、前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記正規条件情報生成工程により生成された正規条件情報を正規条件情報記憶部に格納する正規条件情報格納工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程とをさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項2に記載のサー

ビス不能攻撃防御方法。

- [8] 前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に通知するシグネチャ通知工程と、前記中継装置が前記シグネチャ通知工程により通知された容疑シグネチャおよび正規シグネチャに基づいてパケットの通過を制限制御するパケット制限制御工程とをさらに含んだことを特徴とする請求項7に記載のサービス不能攻撃防御方法。
- [9] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、  
前記ネットワークから受信されたパケットによる攻撃を前記ゲート装置が検知する攻撃検知工程と、  
前記攻撃検知工程により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が前記中継装置から取得する正規アドレス情報取得工程と、  
前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御を前記ゲート装置がおこなう通過制御工程とを含んだことを特徴とする請求項1に記載のサービス不能攻撃防御方法。
- [10] 前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを前記ゲート装置が生成する容疑シグネチャ生成工程をさらに含み、  
前記正規アドレス情報取得工程は、  
前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする請求項9に記載のサービス不能攻撃防御方法。
- [11] 前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条

件情報生成工程と、前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする請求項10に記載のサービス不能攻撃防御方法。

- [12] 前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報生成工程により生成された正規条件情報に示される条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、

前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項11に記載のサービス不能攻撃防御方法。

- [13] 前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に転送するシグネチャ転送工程をさらに含んだことを特徴とする請求項12に記載のサービス不能攻撃防御方法。

- [14] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、

前記ゲート装置は、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、

前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、

前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段と

を備えたことを特徴とするサービス不能攻撃防御システム。

- [15] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器と

の間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、

前記ゲート装置は、

前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、

前記攻撃検知手段により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手段と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とするサービス不能攻撃防御システム。

- [16] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置であって、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、

前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、

前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段と

を備えたことを特徴とするゲート装置。

- [17] 前記正規アドレス情報取得手段は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手段と、前記アドレス情報通知手段により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手段とを備えたことを特徴とする請求項16に記載のゲート装置。

- [18] 前記正規アドレス情報取得手段は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情

報送信要求手段と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手段とを備えたことを特徴とする請求項17に記載のゲート装置。

- [19] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置であって、

前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、

前記攻撃検知手段により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手段と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とするゲート装置。

- [20] 前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段をさらに備え、

前記正規アドレス情報取得手段は、

前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする請求項19に記載のゲート装置。

- [21] 前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段と備えたことを特徴とする請求項20に記載のゲート装置。

- [22] サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、

前記ゲート装置のアドレス情報を取得するアドレス情報取得手段と、  
前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手段により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手段と  
を備えたことを特徴とする中継装置。

- [23] サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、

前記ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、

前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段と

を備えたことを特徴とする中継装置。

- [24] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置に用いるゲート装置用プログラムであって、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手順と、

前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、

前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順と

をコンピュータに実行させることを特徴とするゲート装置用プログラム。

- [25] 前記正規アドレス情報取得手順は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手順と、前記アドレス情報通知手順により通知した自装

置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手順とを含んだことを特徴とする請求項24に記載のゲート装置用プログラム。

- [26] 前記正規アドレス情報取得手順は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手順と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手順とを含んだことを特徴とする請求項24に記載のゲート装置用プログラム。

- [27] ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するゲート装置に用いるゲート装置用プログラムであって、

前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手順と、

前記攻撃検知手順により前記通信機器への攻撃が検知された場合に、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を前記中継装置から取得する正規アドレス情報取得手順と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手順と

をコンピュータに実行させることを特徴とするゲート装置用プログラム。

- [28] 前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順をさらに含み、

前記正規アドレス情報取得手順は、

前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得することを特徴とする請求項27に記載のゲート装置用プログラム。

- [29] 前記通過制御手順は、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過

を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする請求項28に記載のゲート装置用プログラム。

- [30] サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、

前記ゲート装置のアドレス情報を取得するアドレス情報取得手順と、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手順により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手順と

をコンピュータに実行させることを特徴とする中継装置用プログラム。

- [31] サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、

前記ネットワークに所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手順と、

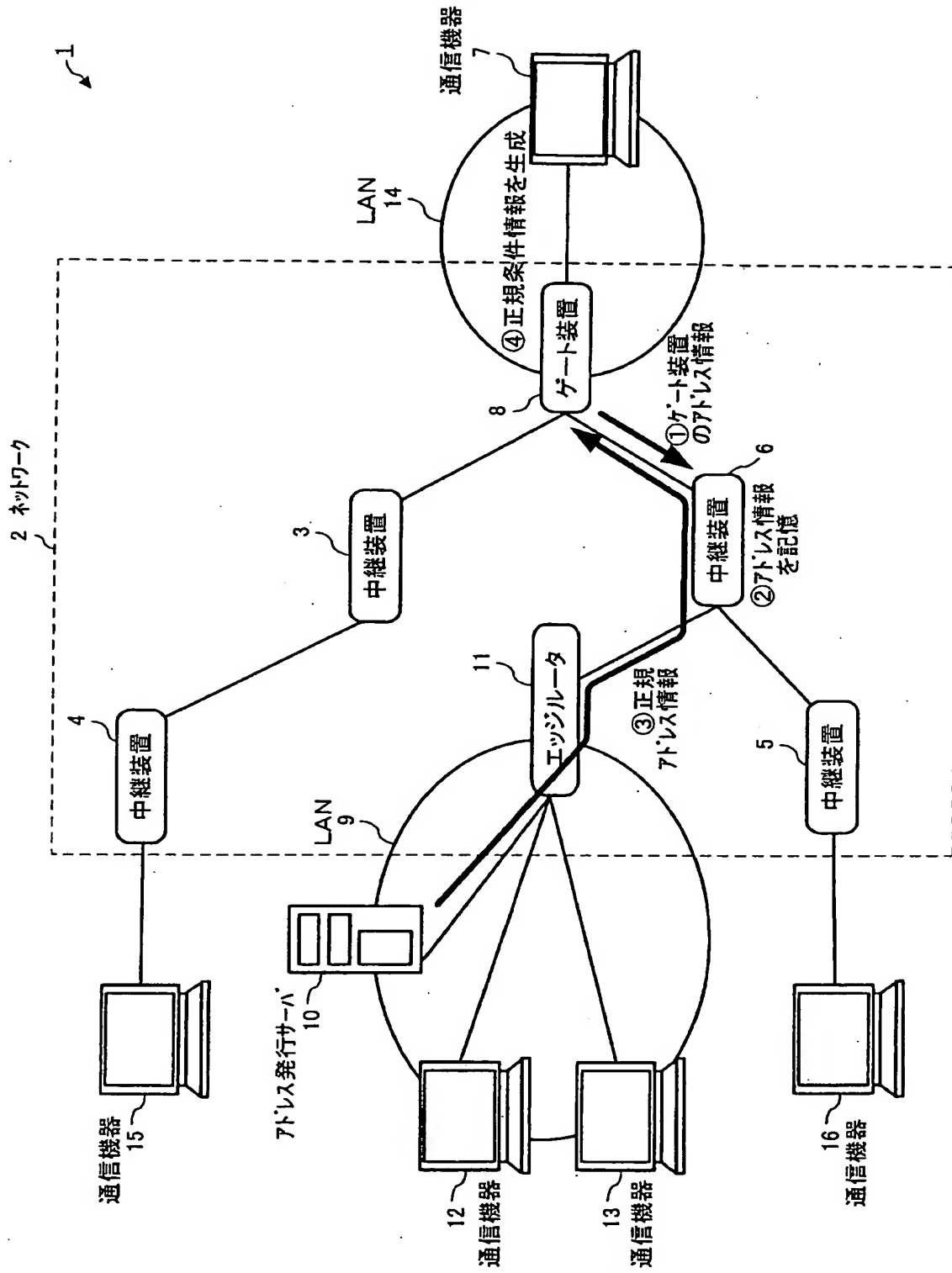
前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手順に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順と

をコンピュータに実行させることを特徴とする中継装置用プログラム。

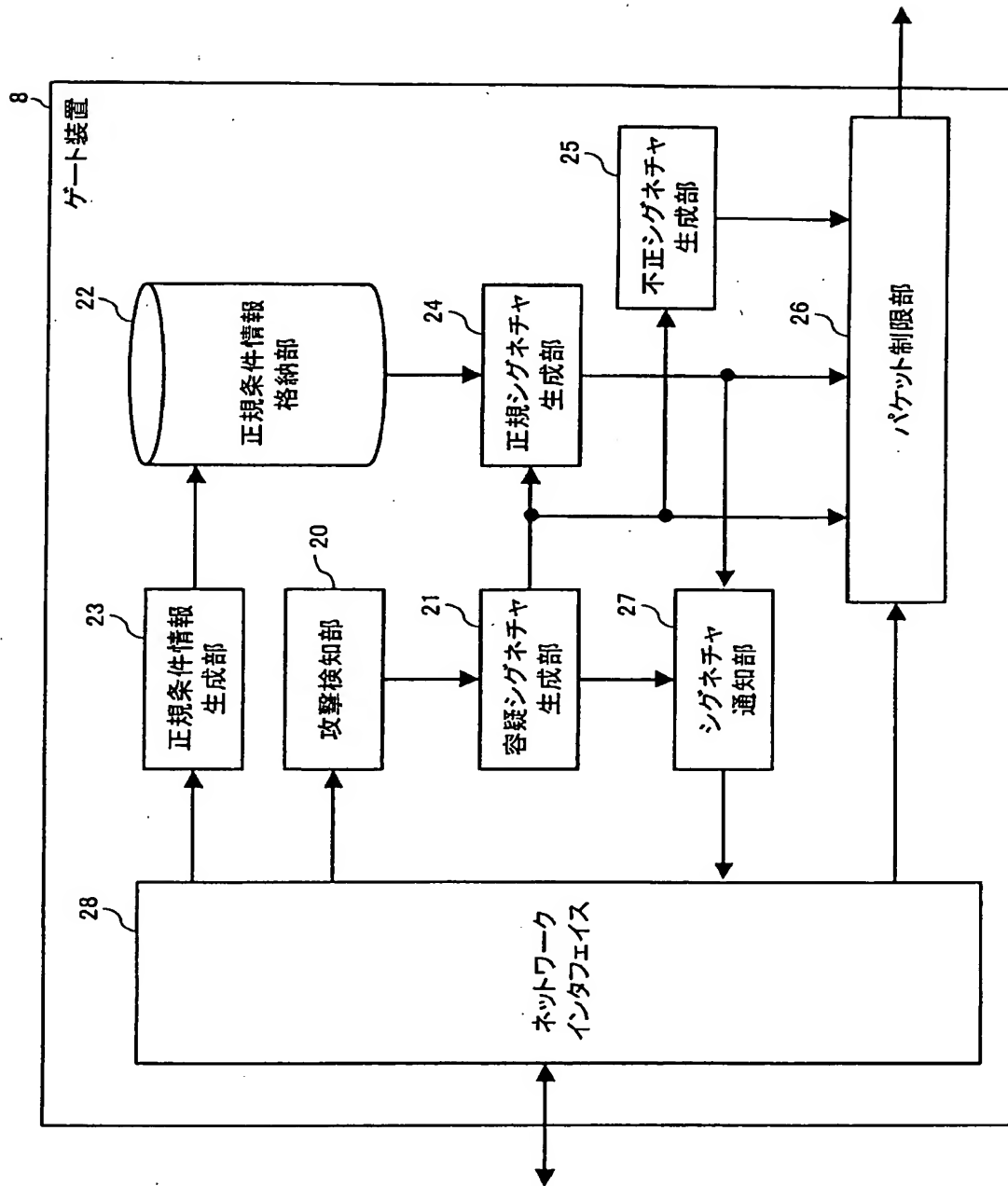
## 要 約 書

ネットワーク2上に所在する正当な装置(アドレス発行サーバ10)により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置8が取得し、取得した正規アドレス情報に基づいてゲート装置8が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器7へ攻撃をおこなうパケットの通過を制限するよう構成する。

[図1]



[図2]



[図3]

	検知属性	検知閾値	検出時間
1	{Dst=192.168.1.1/32, Protocol=TCP, Port=80}	500kbps	10秒
2	{Dst=192.168.1.2/32, Protocol=UDP}	300kbps	10秒
3	{Dst=192.168.1.0/24}	1Mbps	20秒

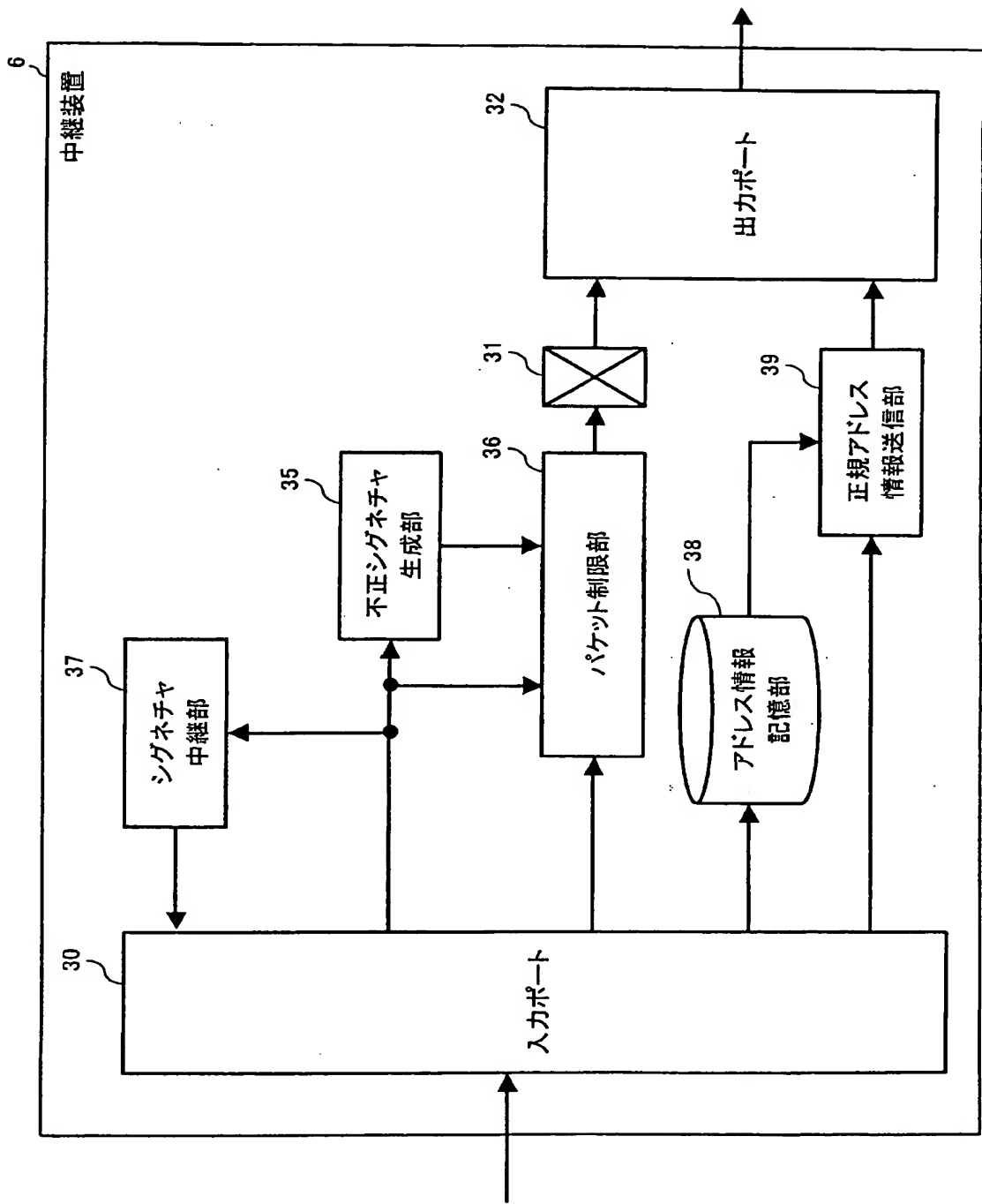
[図4]

	正規条件
1	{Src=172.16.10.0/24}
2	{TOS=0x01}

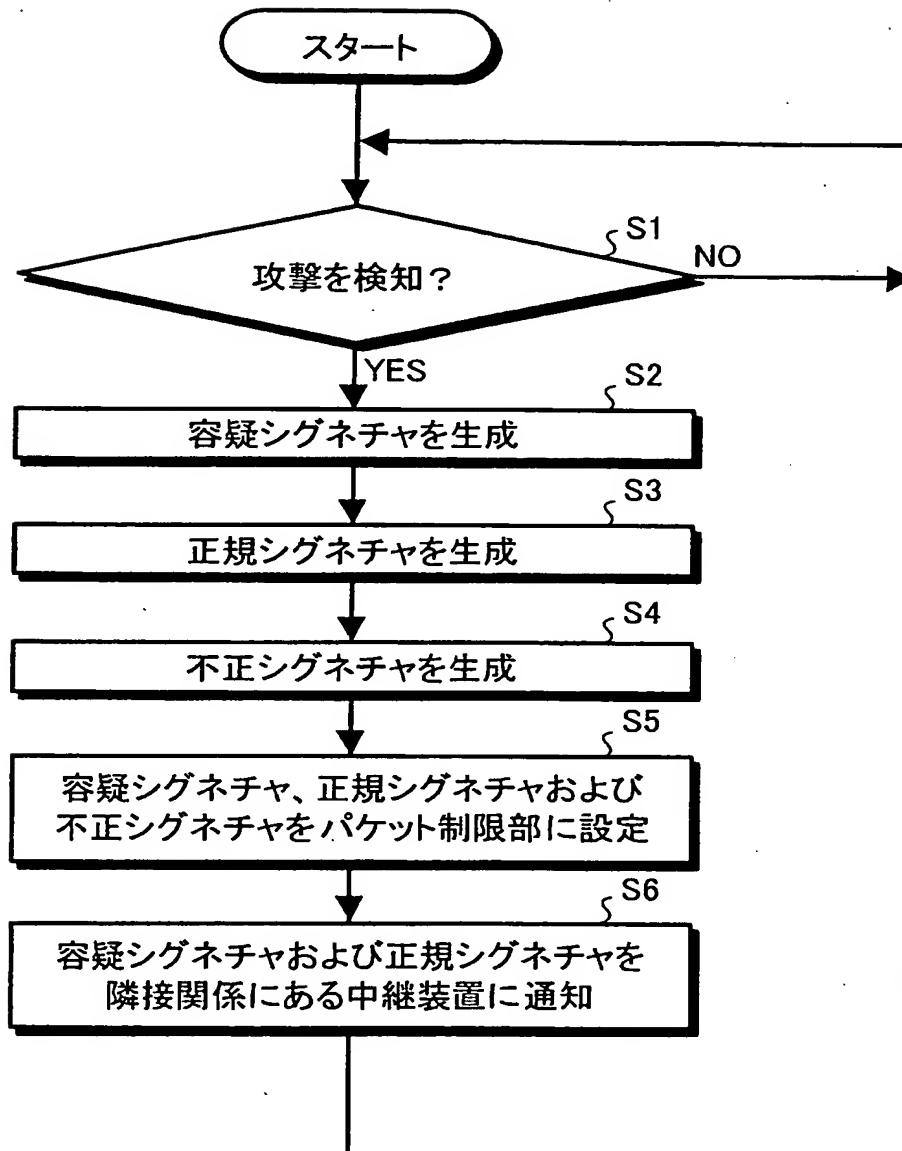
[図5]

	不正条件
1	500kbps以上のパケットが30秒以上連続送信されている
2	300kbps以上のICMP/Echo Replyパケットが15秒以上連続送信されている
3	300kbps以上のフラグメントパケットが15秒以上連続送信されている

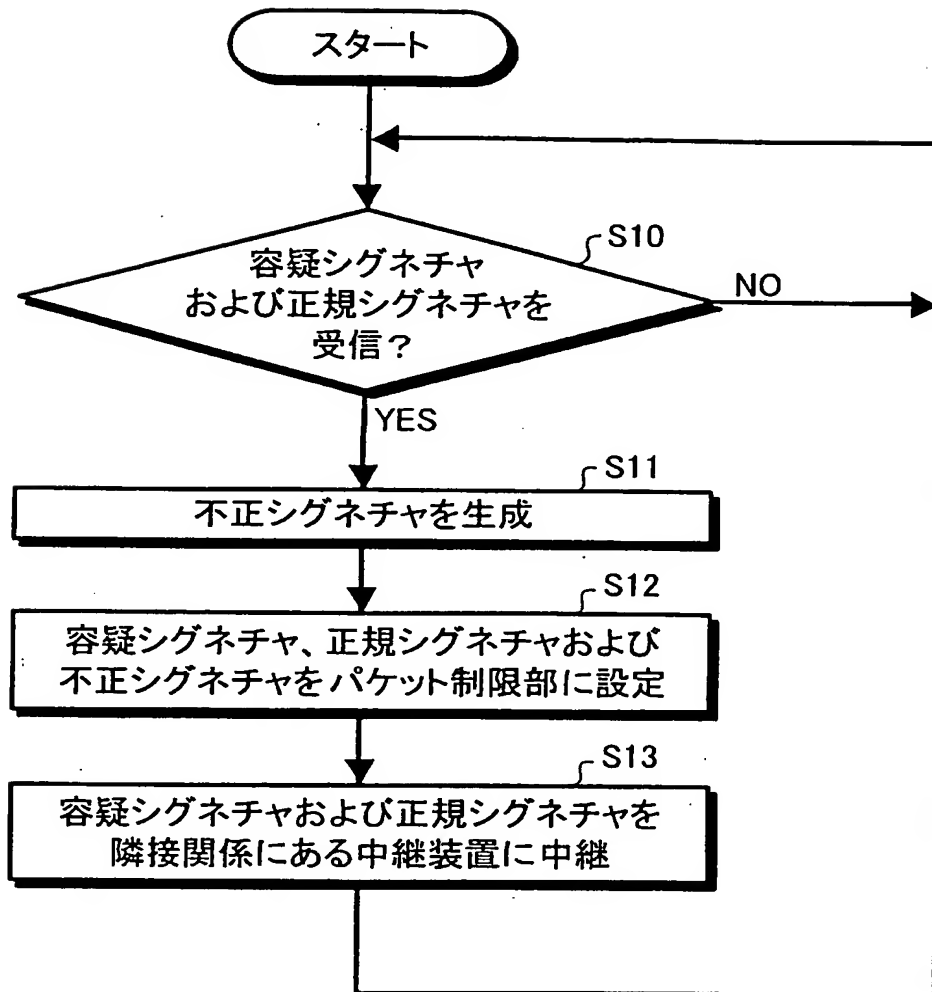
[図6]



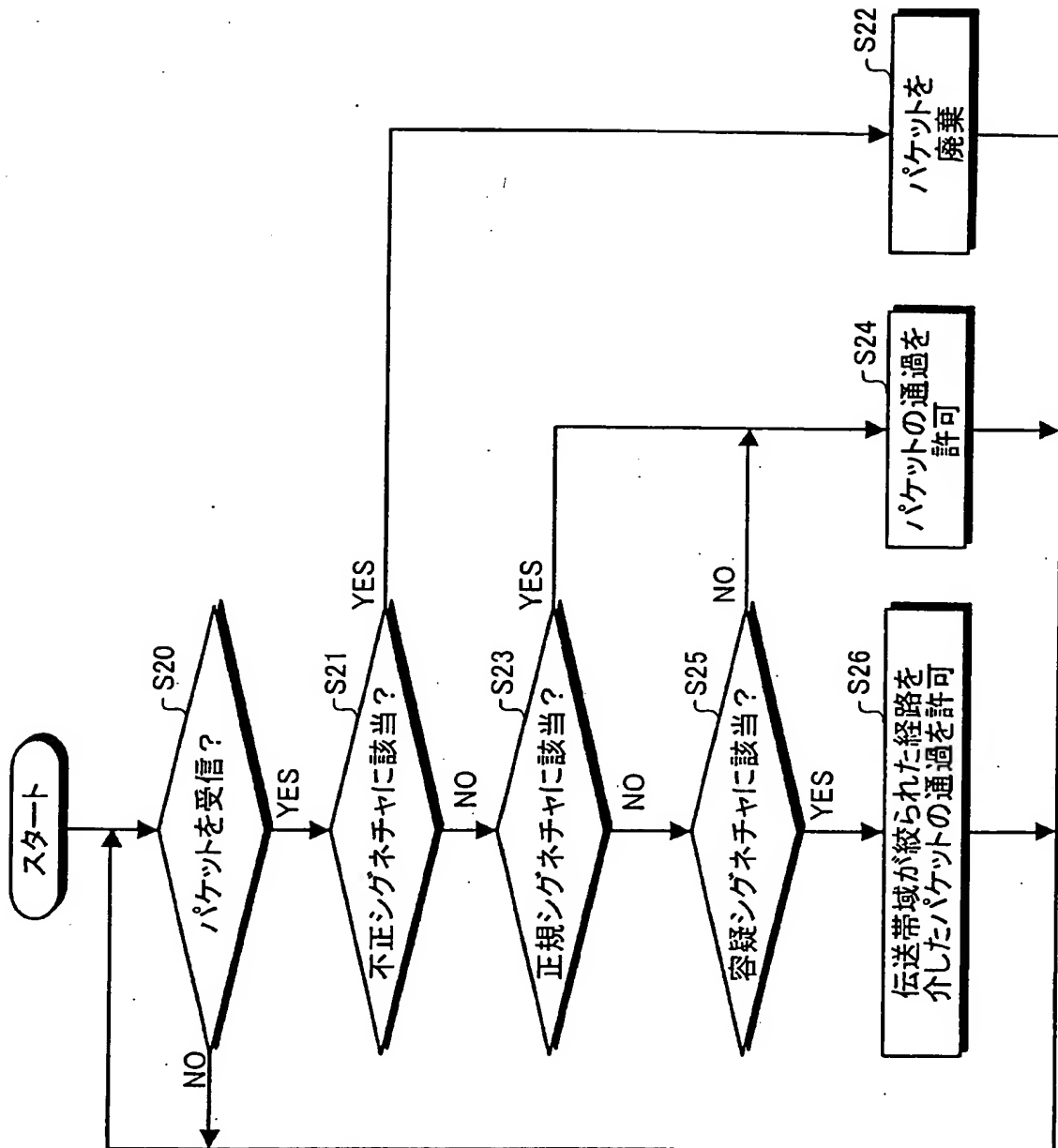
[図7]



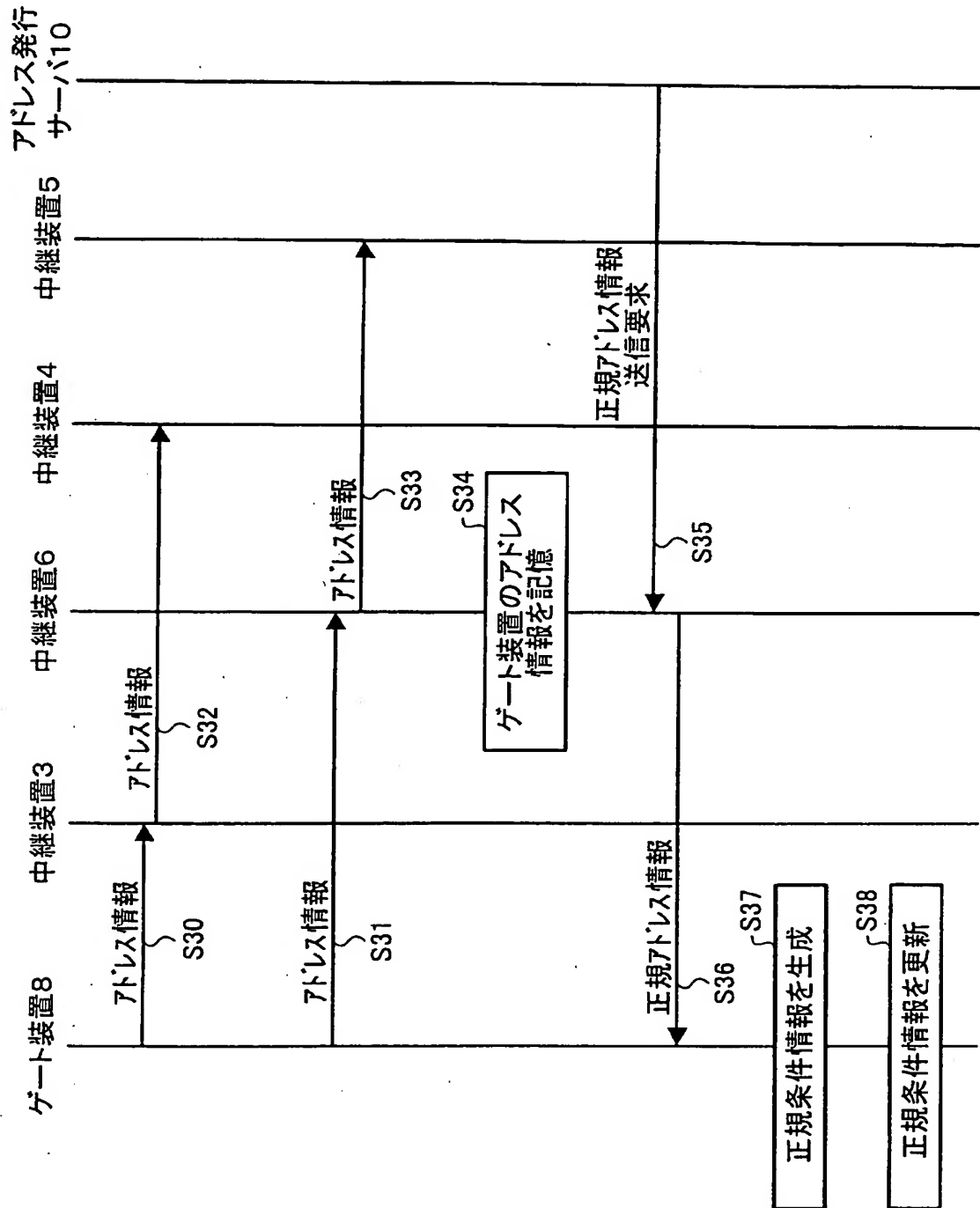
[図8]



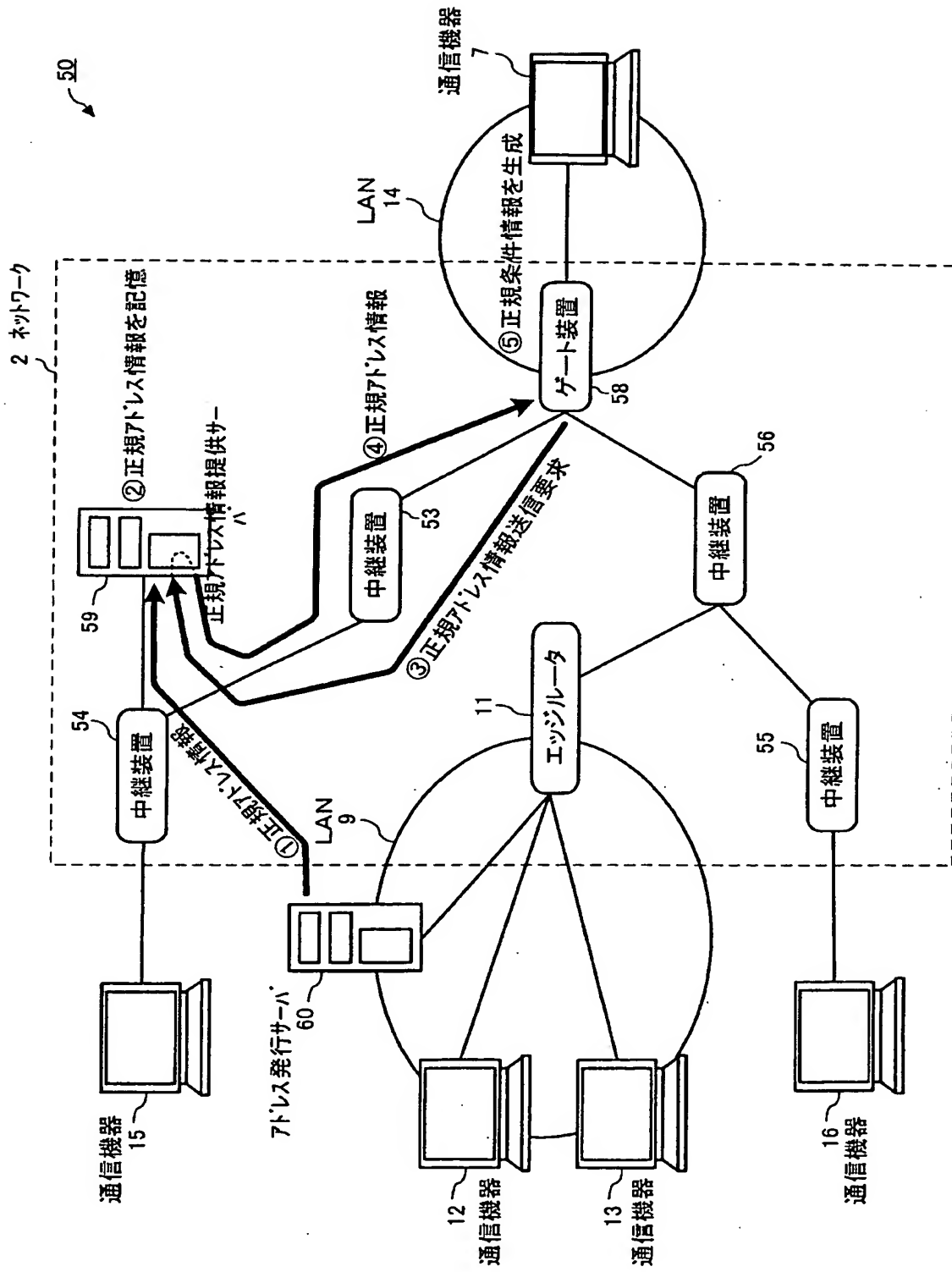
[図9]



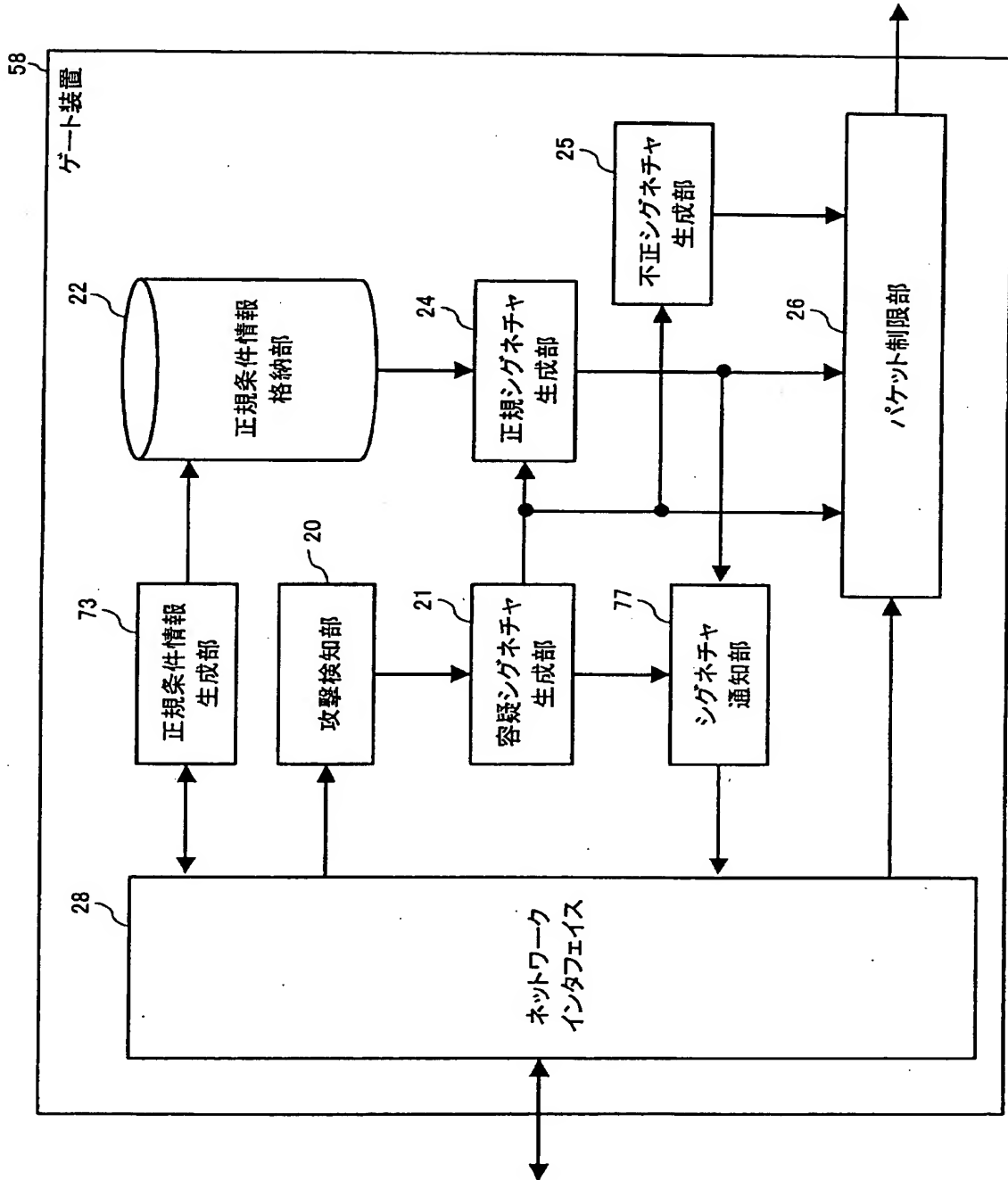
[図10]



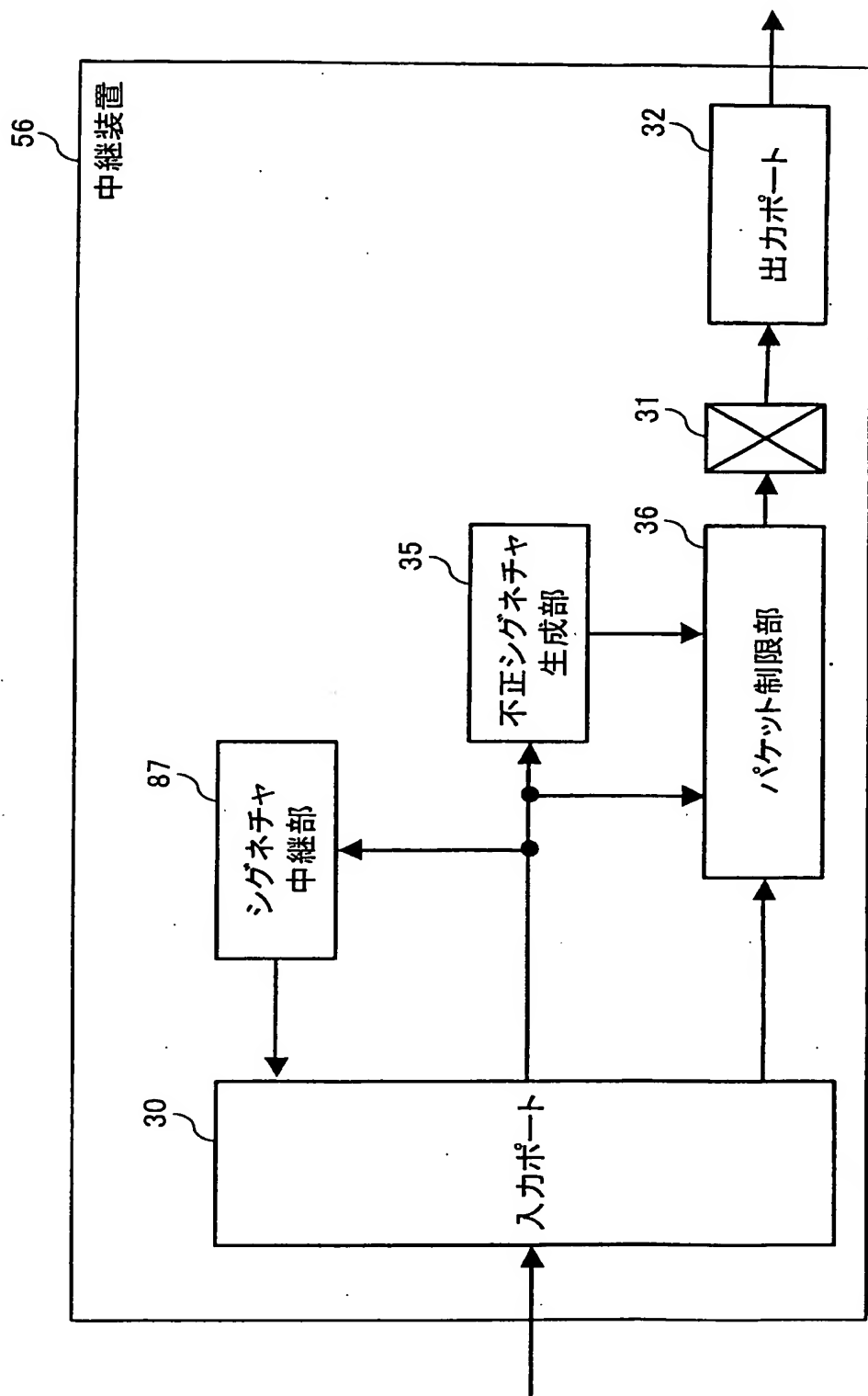
[図11]



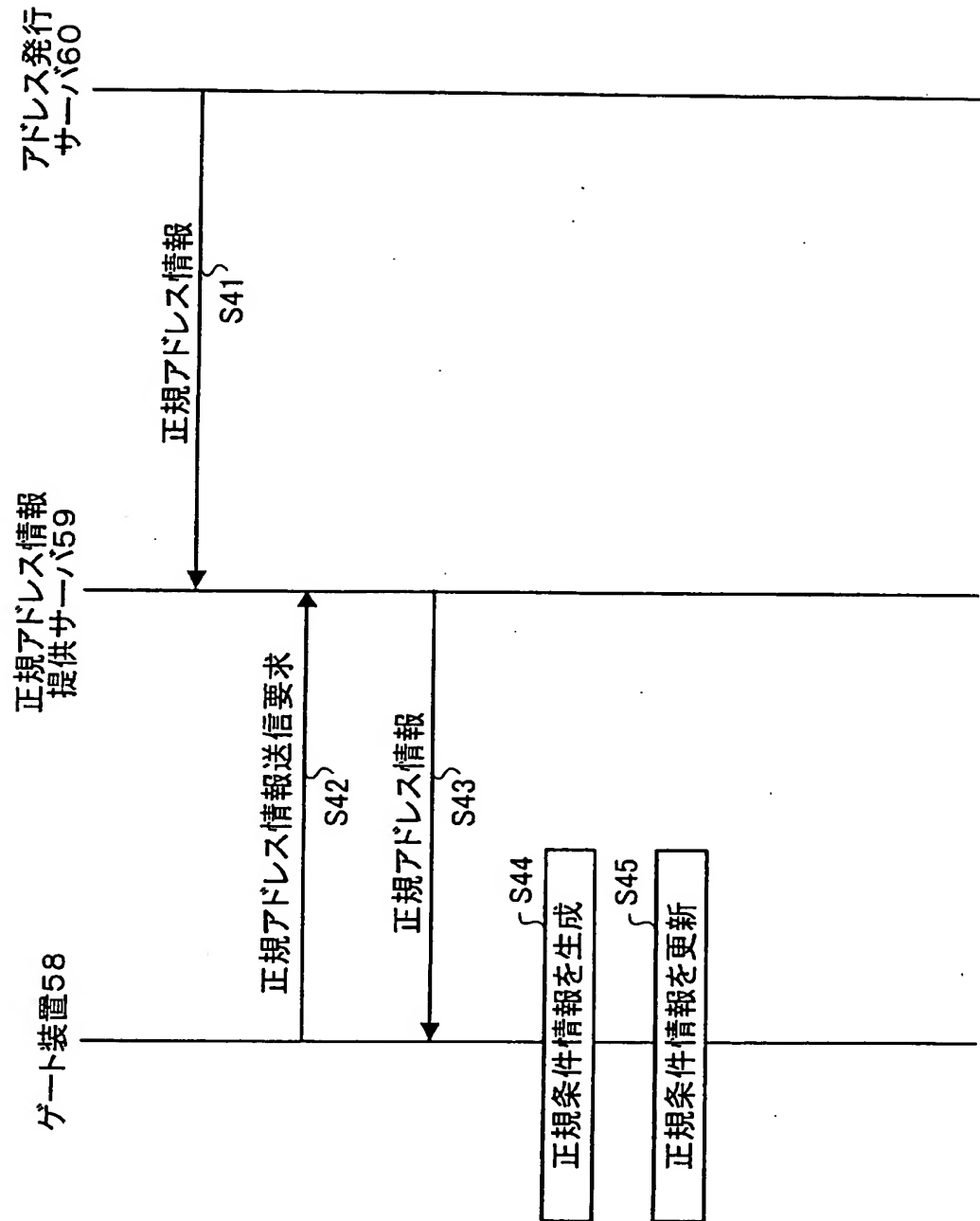
[図12]



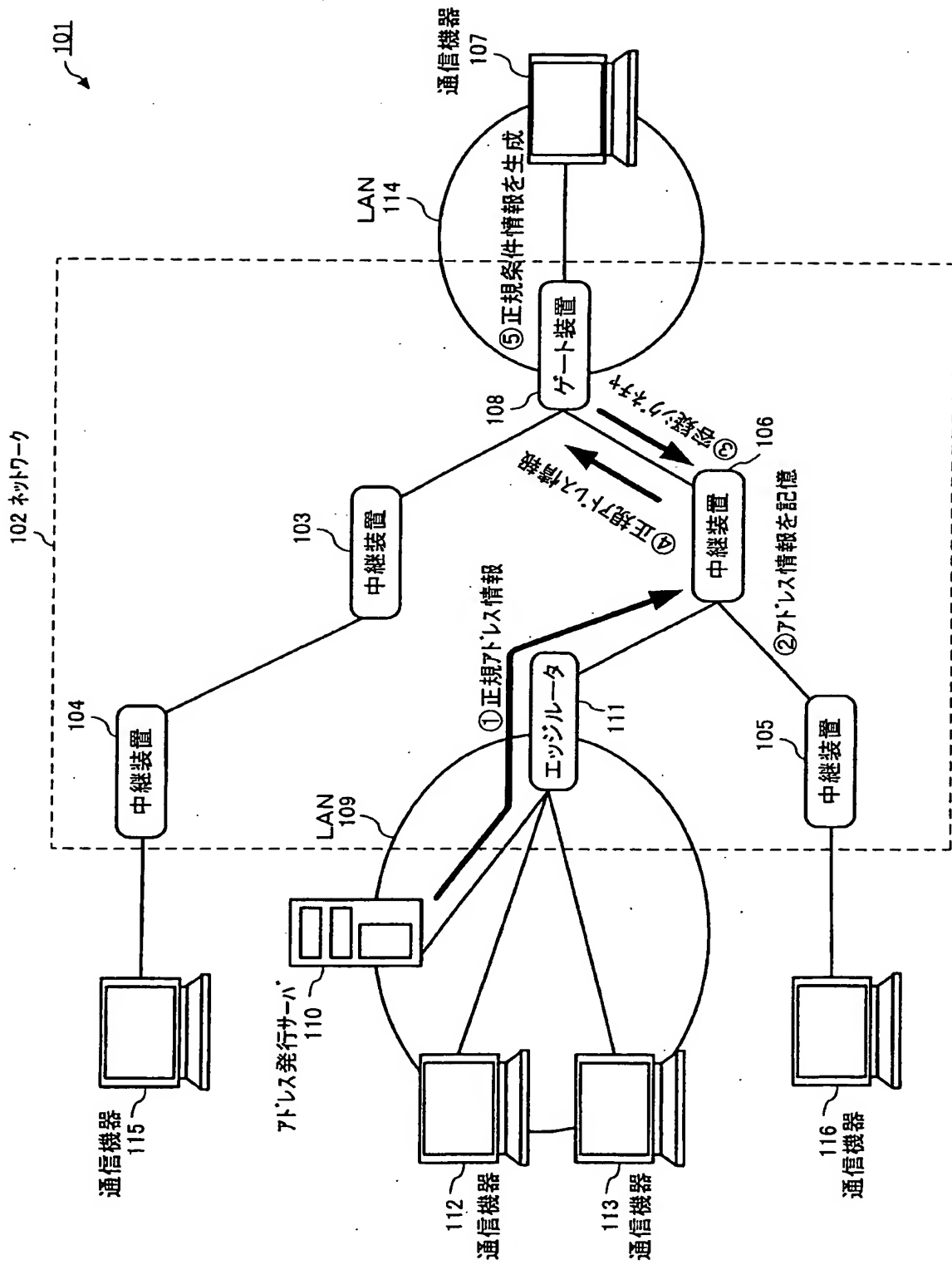
[図13]



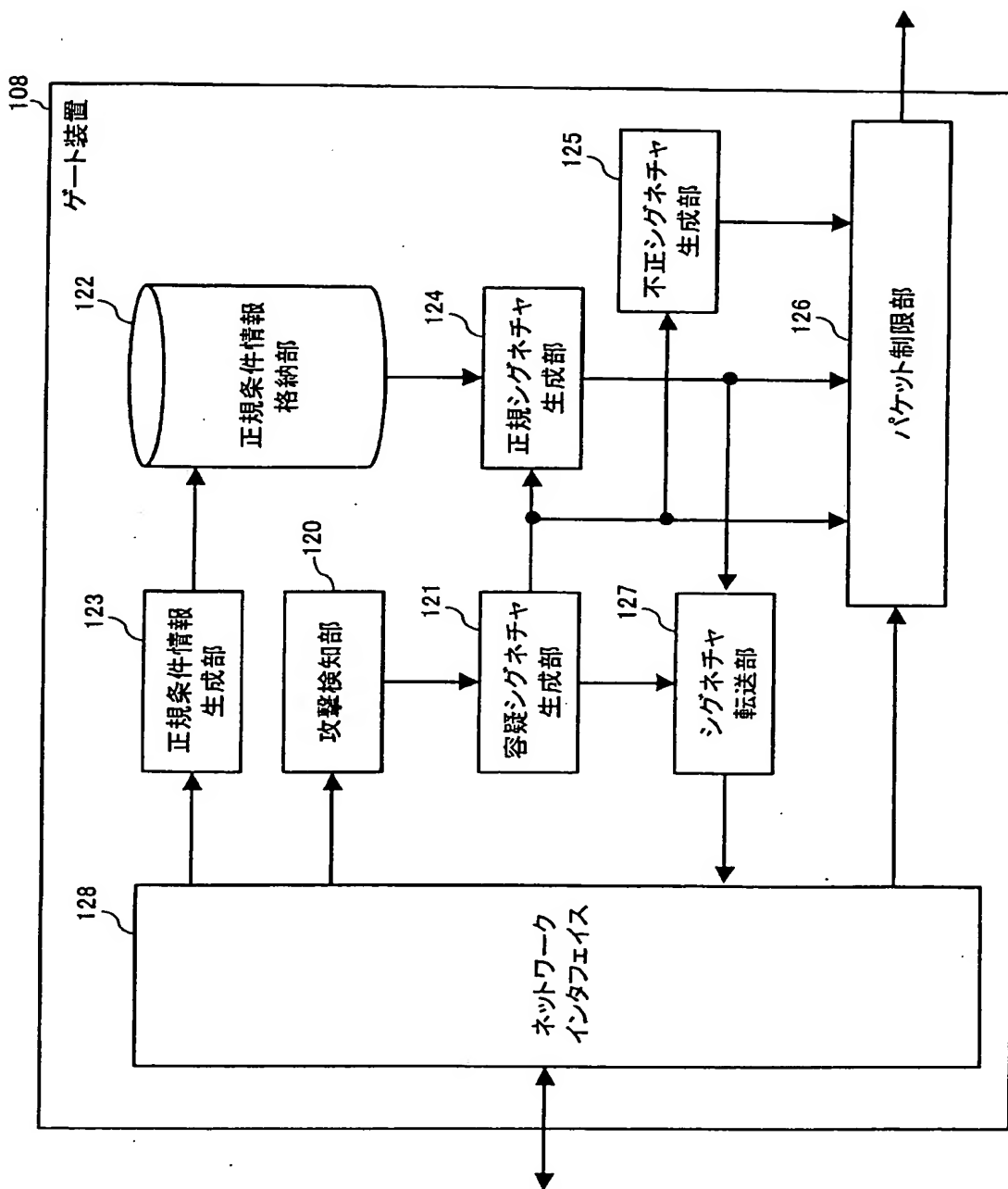
[図14]



[図15]



[図16]



[図17]

	検知属性	検知閾値	検出時間
1	{Dst=192.168.1.1/32, Protocol=TCP, Port=80}	500kbps	10秒
2	{Dst=192.168.1.2/32, Protocol=UDP}	300kbps	10秒
3	{Dst=192.168.1.0/24}	1Mbps	20秒

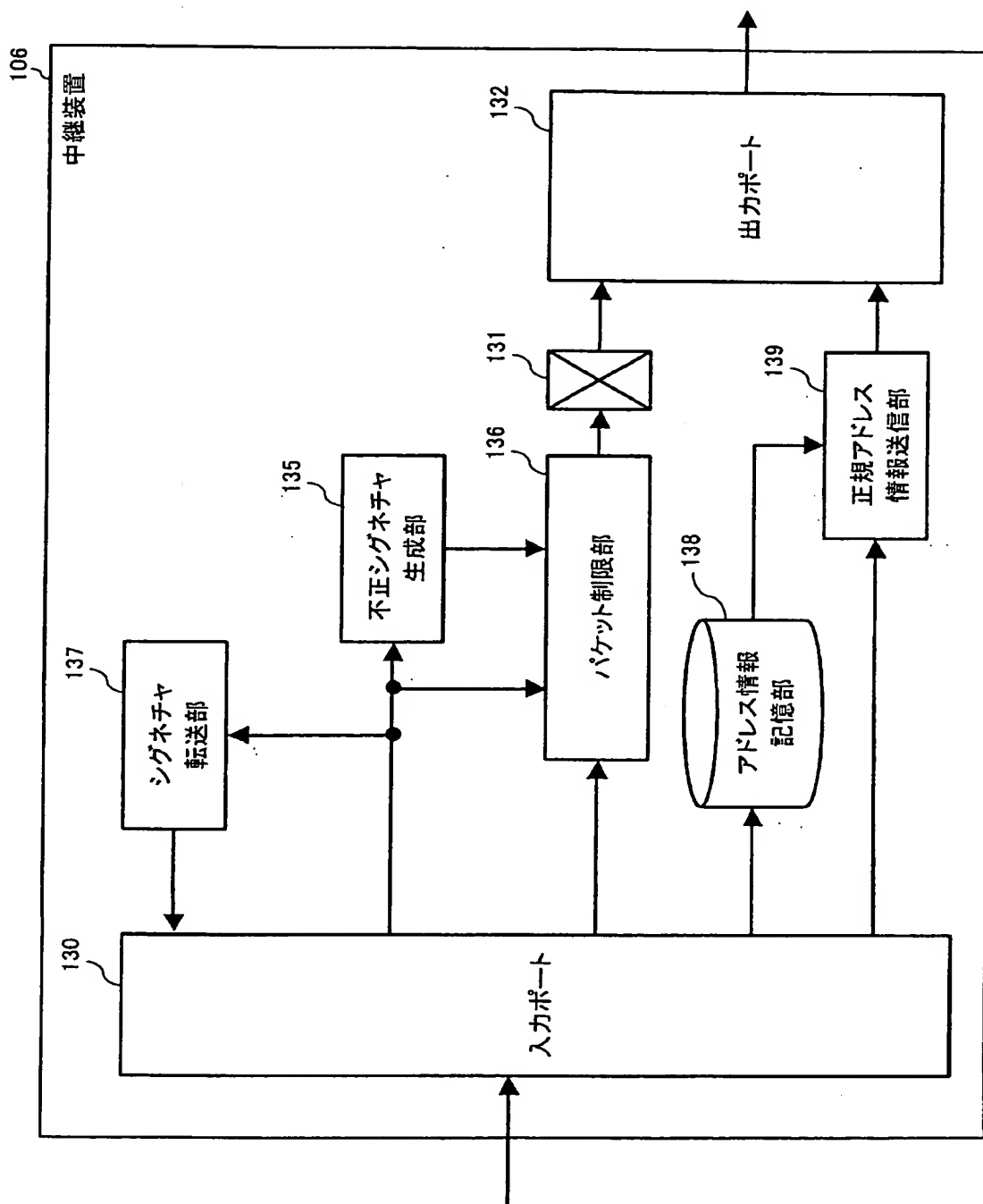
[図18]

	正規条件
1	{Src=172.16.10.0/24}
2	{TOS=0x01}

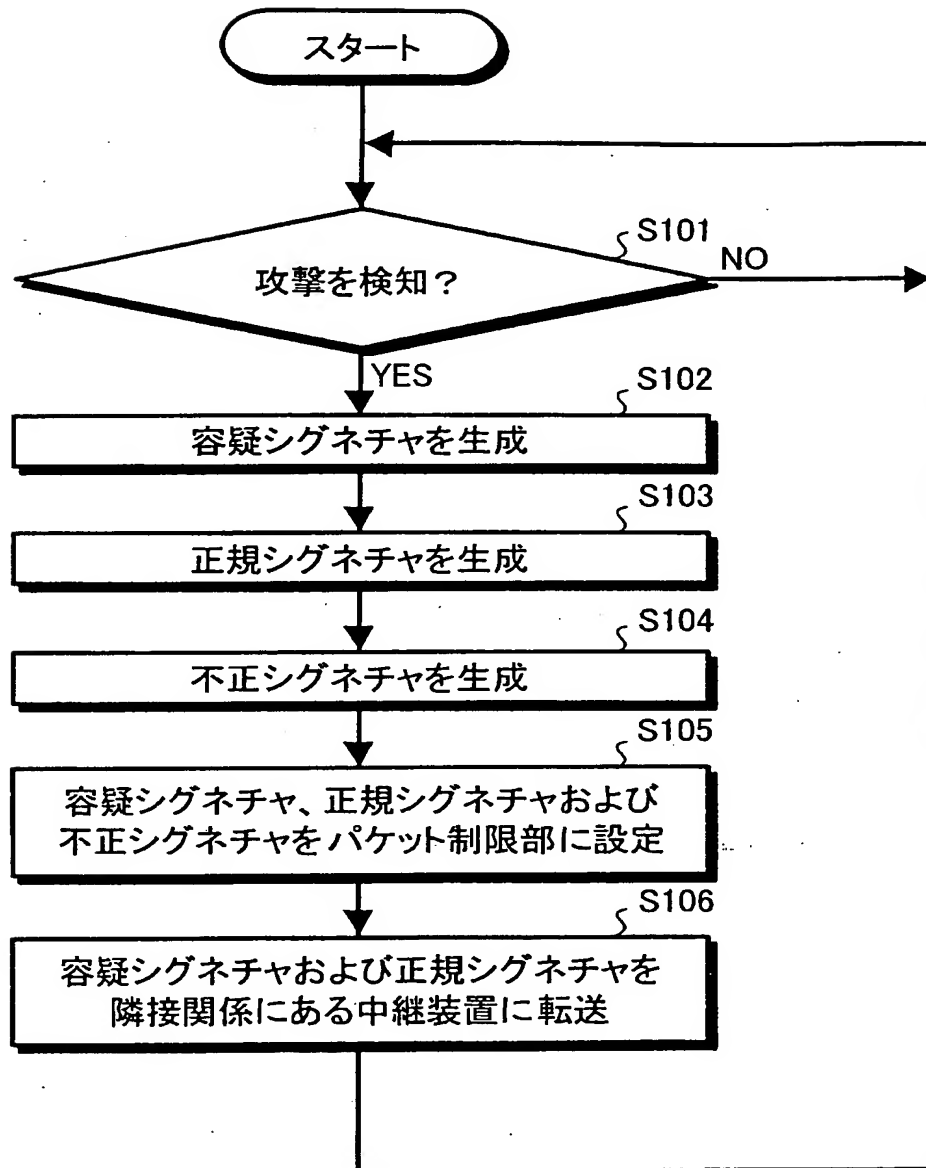
[図19]

	不正条件
1	500kbps以上のパケットが30秒以上連続送信されている
2	300kbps以上のICMP/Echo Replyパケットが15秒以上連続送信されている
3	300kbps以上のフラグメントパケットが15秒以上連続送信されている

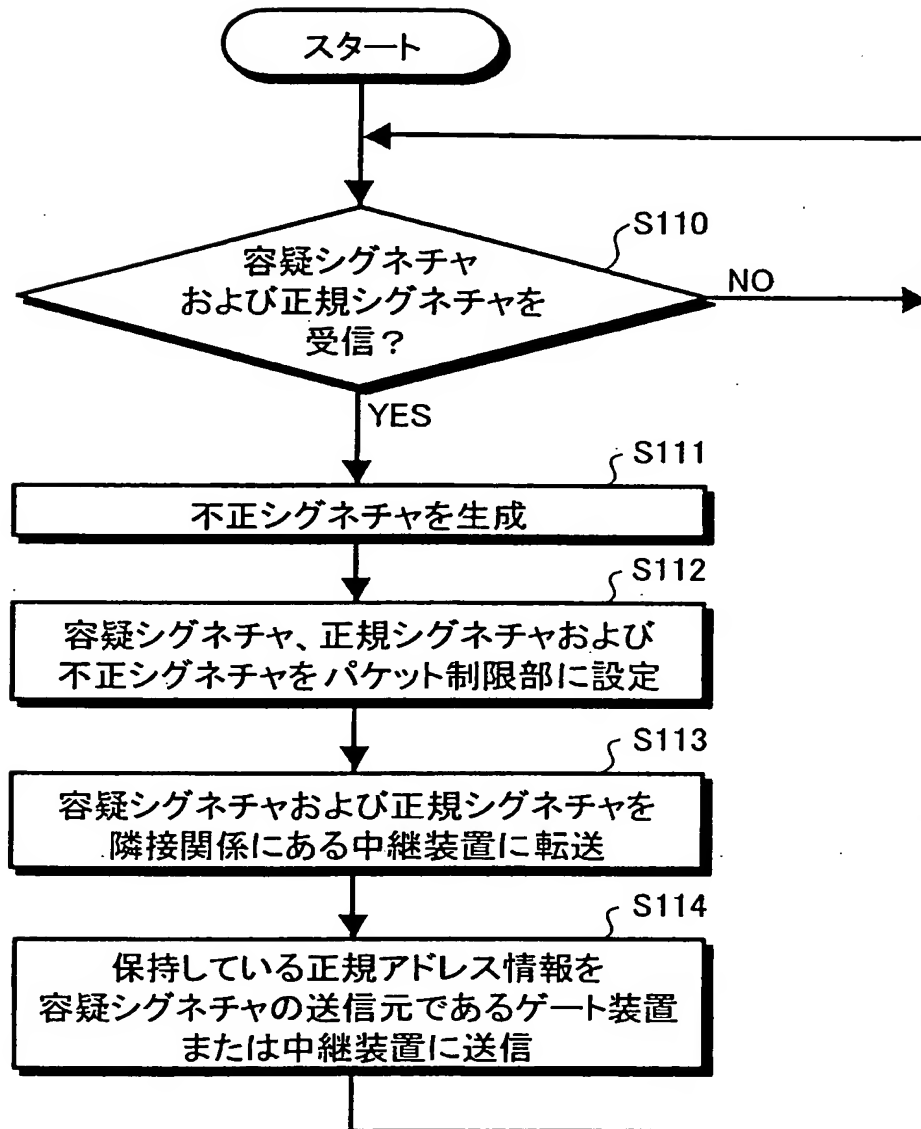
[図20]



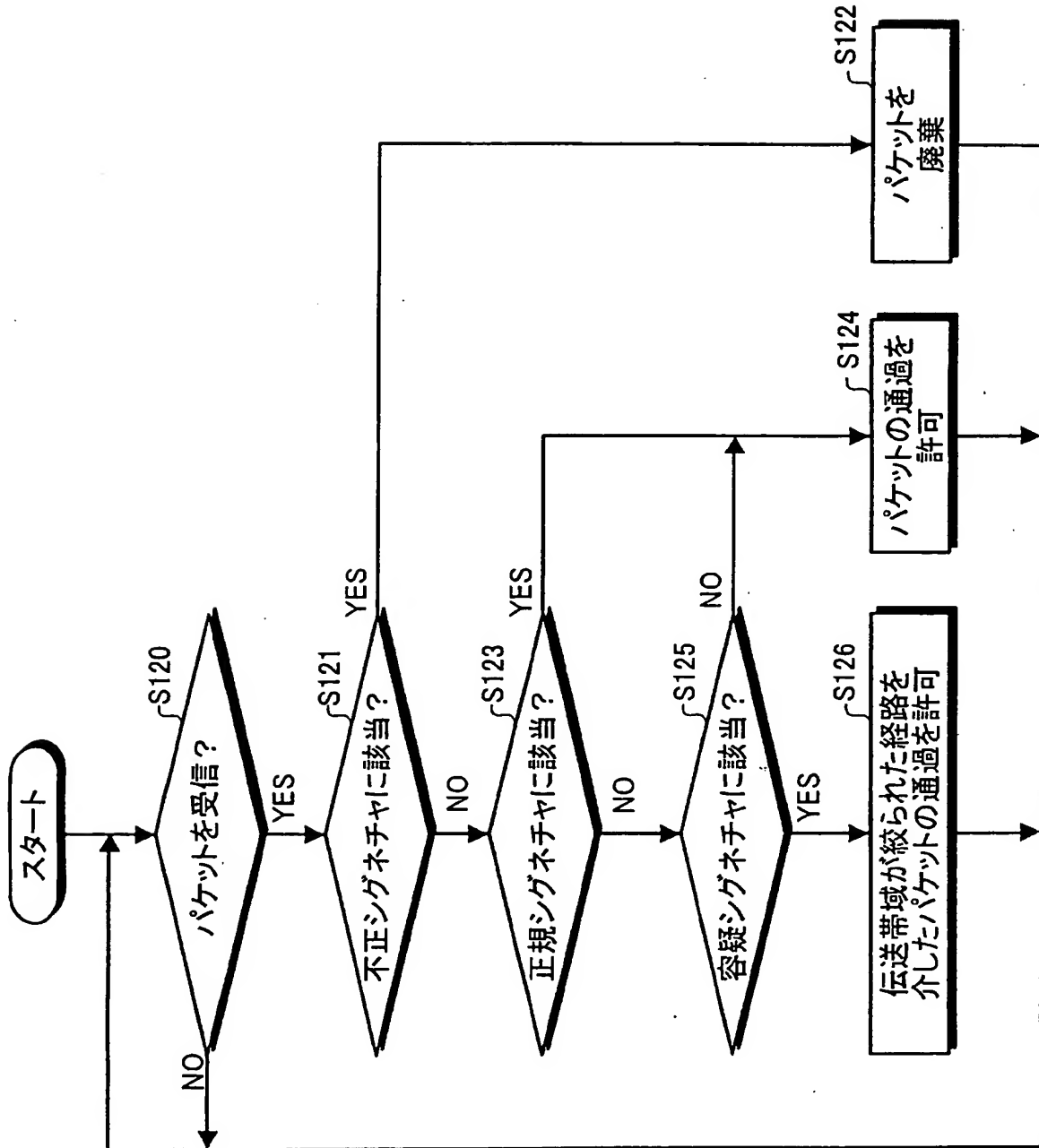
[図21]



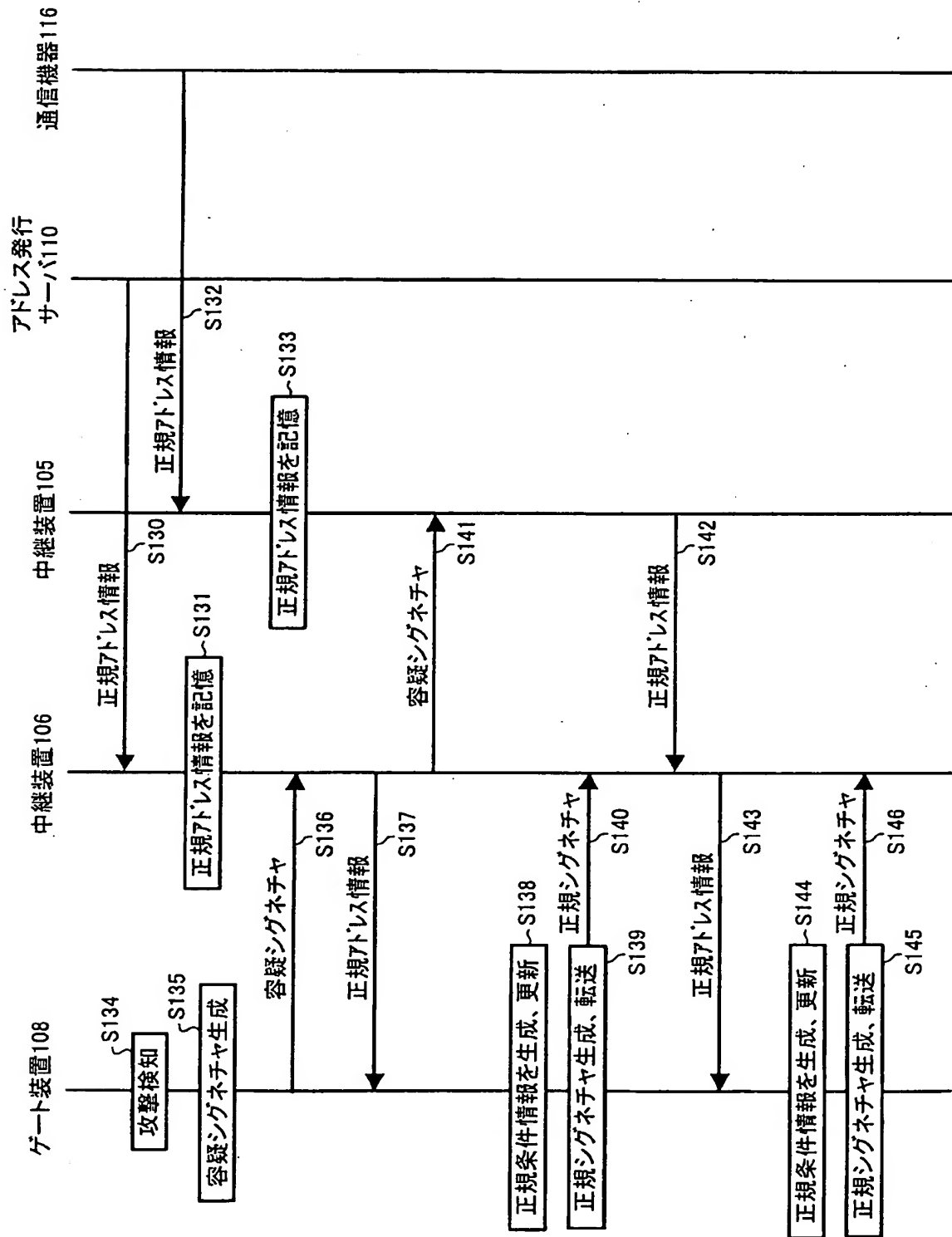
[図22]



[図23]



[図24]



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**